LITE DEPALMA GREENBERG & AFANADOR, LLC
Joseph J. DePalma
Catherine B. Derenze
570 Broad Street, Suite 1201
Newark, New Jersey 07102
Telephone: (973) 623-3000
Facsimile: (973) 623-0858
jdepalma@litedepalma.com
cderenze@litedepalma.com

[*Additional Attorneys on Signature Page*]

Attorneys for Plaintiffs & the Proposed Classes

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

In re CityMD Data Privacy Litigation	Civil Action No.: 2:24-cv-06972-JXN-CLW

CONSOLIDATED CLASS ACTION COMPLAINT

V.A. and T.G. bring this consolidated class action lawsuit on behalf of themselves and all others similarly situated, by and through undersigned counsel, and hereby allege the following against Defendant Summit Health Management LLC d/b/a CityMD ("Summit Health" or "CityMD").[1] Facts pertaining to Plaintiffs and their experiences and circumstances are alleged based upon personal knowledge, and all other facts alleged herein are based upon investigation of their counsel and, where indicated, upon information and good faith belief.

[1] By Order entered on December 17, 2024, the Court consolidated *T.G. v. Summit Health Management, LLC*, Case No. 2:24-cv-6972 and *V.A. v. Summit Health Management, LLC*, Case No. 2:24-cv-9039 into the first filed action, *T.G. v. Summit Health Management, LLC*, Case No. 2:24-cv-6972. *See* Dkt No. 63.

NATURE OF THE ACTION

1. Information concerning a person's physical and mental health is among the most confidential and sensitive information in our society and the mishandling of such information can have serious consequences including, but certainly not limited to, discrimination in the workplace and/or denial of insurance coverage.[2]

2. Simply put, if people do not trust that their protected health information will be kept private and secure, they may be less likely to seek medical treatment which can lead to much more serious health consequences down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to any unauthorized entities is vitally necessary to maintain public trust in the healthcare system as a whole.

3. The need for data privacy, security and transparency is particularly acute when it comes to the rapidly expanding world of digital telehealth providers; of all the information the average internet user shares with technology companies, health data is some of the most extensive, valuable and controversial.[3]In 2019, Summit Health Management, LLC and CityMD, a leading

[2] *See* Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world* (Nov. 16, 2022), https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ ("While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it's even more verboten in addiction treatment, as patients' medical history can be inherently criminal and stigmatized."); *see also* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites* (June 16, 2022), https://themarkup.org/pixelhunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited Jan. 12, 2025).

[3] Protected and highly sensitive medical information collected by telehealth companies includes many categories from intimate details of an individual's conditions, symptoms, diagnoses and treatments to personally identifying information to unique codes which can identify and connect individuals to the collecting entity. *See* Molly Osberg & Dhruv Mehrotral, *The Spooky, Loosely Regulated World of Online Therapy*, JEZEBEL (Feb. 19, 2020), https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137 (last visited Jan. 13, 2025).

urgent care provider in the New York metro area, finalized a merger agreement that created a single entity, known as Summit Health.[4] As a result of the merger, Summit Health Management controls and/or operates over 400 urgent care and other medical clinics as well as telemedicine services throughout the New York City metropolitan area, parts of upstate New York and Long Island, Pennsylvania, New Jersey, and parts of Oregon that operate under the "CityMD" tradename.

4. Plaintiffs bring this class action lawsuit to address CityMD's illegal and widespread practice of disclosing its patients' confidential personally identifiable information ("PII") and protected health information ("PHI," and together with PII collectively referred to as "Private Information") to unauthorized third-party advertisers including, but not limited to, Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta"), Google LLC ("Google"), and LinkedIn Corporation ("LinkedIn"). [5]

5. In order to market, sell and provide its medical services, CityMD owns, maintains and controls www.citymd.com and its webpages (the "Website"), which Defendant encourages its patients to use to (i) book medical appointments, (ii) locate urgent care facilities, (iii) pay bills,

[4] *See CityMD and Summit Health Finalize Merger* (Aug. 13, 2019), https://www.summithealth.com/news/citymd-and-summit-health-finalize-merger (last visited Jan. 12, 2025).

[5] This Complaint contains images and evidence demonstrating that certain trackers such as the Meta Pixel were used on Defendant's Website, but Plaintiffs (without the benefit of discovery) do not have access to every tracking tool that was previously installed on the Website, including for example Facebook Conversions API, that operates server-side. Plaintiffs' research indicates that Defendant also utilized at least the following trackers: Microsoft Universal Events (Bing tracker), Siteimprove, Datadog, Salesforce Marketing Personalization (Evergage), The Trade Desk, and BlueCava/Adstra on its Website.

(iv) check insurance coverage, (v) research treatment options and (vi) research specific medical conditions.[6]

6. Defendant represents to its patients that "*[w]hen you browse [the CityMD] website, you do so anonymously … We do not collect personal information for the purpose of reselling or distributing that information*."[7]

7. Despite and contrary to these representations, CityMD collects patients' and prospective patients' Private Information and discloses it to third-party advertisers who use it to target the Website users with advertisements related to the users' medical conditions, treatments sought from CityMD, and other related goods and/or services.

8. Defendant's illegal privacy violations occurred and continue to occur because of the tracking technologies that it installed on its Website including, but not limited to, the Meta Pixel, Google Analytics, Google DoubleClick, LinkedIn Insight Tag, and related tracking tools (collectively, "Tracking Technologies").

9. The Tracking Technologies that Defendant installed and configured allowed unauthorized third parties to intercept the contents of patient communications, view patients' Private Information, mine that information for purposes unrelated to the provision of healthcare and further monetize it to deliver targeted advertisements to specific individuals.

10. In doing so, and by designing its Website in the manner described herein, CityMD knew or should have known that its patients would use the Website to communicate Private Information while obtaining and receiving medical services.

---

[6] https://www.citymd.com/services/illnesses (last visited Jan. 12, 2025).

[7] *Privacy policy*, https://www.citymd.com/privacy (emphasis added) (last visited Jan. 12, 2025).

11. Operating as designed and as implemented by Defendant, the invisible Tracking Technologies allowed the Private Information that Plaintiffs and Class Members submitted to Defendant to be unlawfully disclosed to Facebook, Google, LinkedIn and likely other third parties alongside Plaintiffs' and Class Members' unique and persistent IDs, IP addresses and other static identifiers in violation of HIPAA, state laws, industry standards and patient expectations.[8]

12. The process of adding third-party Tracking Technologies to webpages is a multi-step process that must be undertaken *by the website owner*.

13. By installing and configuring Tracking Technologies on its Website, Defendant effectively planted a bug in Plaintiffs' and Class Members' web browsers that caused their communications to be intercepted, accessed, viewed and captured by third parties in real time, as they were communicated by patients based on the parameters Defendant chose to implement.

14. Upon information and good faith belief, CityMD also installed and implemented Conversions API on its servers.

15. Conversions API serves the same purpose as the Tracking Technologies on the Website in that it collects and transmits Private Information to, for example, Facebook. Unlike the Meta Pixel, however, Conversions API functions from CityMD's servers and therefore cannot be stymied by the use of anti-pixel software or other workarounds.[9]

---

[8] While the Meta Pixel as well as other trackers may be small (and, in fact, invisible pieces of code), the data they collect and transmit is extremely extensive. *See Meta for Developers: Meta Pixel*, https://developers.facebook.com/docs/meta-pixel/ (last visited Jan. 14, 2025).

[9] While there is no way to confirm with certainty that a web host like CityMD has implemented Conversions API without access to the host server, companies like Facebook instruct web hosts to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows CityMD "to share website events [with Facebook] that the pixel may lose." *See Best Practices for Conversions API,* https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited Jan. 14, 2025).

16. Upon information and belief, CityMD also installed third-party trackers on its mobile app, available for download to patients and prospective patients, which also collected Users' Private Information and disclosed it to unauthorized data brokers without Users' consent.

17. Plaintiffs and Class Members used Defendant's Website to submit information related to their health conditions or potential health conditions including, for example, searches for specific medical treatments and the booking of medical appointments for their health conditions. Such Private Information allows a third party, such as Facebook or Google, to know that a specific patient was seeking confidential medical care from Defendant as well as the type of medical care being sought.

18. Simply put, the health information disclosed through the Tracking Technologies is personally identifiable.

19. Defendant is a healthcare entity and thus its disclosure of health and medical communications is tightly regulated. HHS has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no health care provider may disclose a person's personally identifiable protected health information to a third party without express written authorization.

20. Healthcare patients simply do not anticipate or expect that their trusted healthcare provider will send PHI or confidential medical information collected via its webpages to a hidden third party—let alone Facebook and Google, which both have a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without the patients' consent. Neither Plaintiffs nor any other Class Members signed a written authorization permitting Defendant to send their Private Information to Facebook or Google.

21. And as noted by the Honorable William J. Orrick in a decision concerning the use of the Meta Pixel by healthcare organizations,

> Our nation recognizes the importance of privacy in general and health information in particular: the safekeeping of this sensitive information is enshrined under state and federal law. The allegations against Meta are troubling: Plaintiff raise potentially strong claims on the merits and their alleged injury would be irreparable if proven.[10]

22. CityMD knew or should have known that by embedding the Tracking Technologies, it was disclosing to third party data brokers sensitive information shared by its Website users, including the PII and PHI of Plaintiffs and Class Members. This is because the Tracking Technologies had to be affirmatively and intentionally placed by Defendant on its Website in order to be used in the way as described herein, *i.e.* to collect and monetize patients' data.

23. To make matters worse, CityMD has ***not*** informed those Users of the unauthorized disclosure of their Private Information, as many other healthcare and telehealth entitles who have utilized similar tracking technology to collect and disclose Private Information to third parties have done.[11]

24. Despite numerous warnings from federal regulators (not to mention several FTC enforcement actions against telehealth companies for similar conduct) about the data privacy risks

---

[10] *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 783 (N.D. Cal. 2022).

[11] In stark contrast to CityMD, in the last year, several medical providers that installed the Meta Pixel on their Web Properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See*, *e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf; Annie Burky, *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies,* FIERCE HEALTHCARE (Oct. 20, 2022), https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3; *Novant Health Notifies Patients of Potential Data Privacy Incident*, PR NEWSWIRE (Aug. 19, 2022), https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html.

of using third-party tracking technologies,[12] CityMD designed and maintained its Website so that Users would be required to submit Private Information in order to participate in health-related services, review treatments offered by CityMD for their medical conditions, make appointments and create accounts, among many other things.

25. The reason CityMD goes to these lengths to obtain this sensitive Private Information is, quite simply, because its Users would ***not*** provide it if they were informed and given a choice. That is, if CityMD told its patients that by using its Website their sensitive Private Information would be collected and disseminated to Facebook and/or other third-party platforms, Users would deny consent and/or demand significant compensation for the use of their private and valuable health information in this manner.

26. As detailed herein, CityMD owes common law, contractual, statutory and regulatory duties to keep Users' Private Information safe, secure and confidential. Furthermore, by obtaining, collecting, using and deriving a benefit from their Private Information, CityMD assumed legal and equitable duties to Users to protect and safeguard their Private Information from unauthorized disclosure.

27. CityMD, however, failed in its obligations and promises by utilizing Tracking Technologies, Conversions API and/or other invisible tracking codes to collect and divulge Users'

[12] *See, e.g.*, Heather Landi, *Regulators Warn Hospitals and Telehealth Companies about privacy risks of Meta, Google Tracking Tech*, FIERCE HEALTHCARE (July 21, 2023), https://www.fiercehealthcare.com/health-tech/regulators-warn-hospitals-and-telehealth-companies-about-privacy-risks-meta-google (last visited June 14, 2024) (noting that the FTC and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) issued a rare joint release announcing that 130 hospital systems and telehealth providers received a letter warning them about the data privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps).

Private Information with unauthorized third parties.[13]

28. Consequently, Plaintiffs bring this action for legal and equitable remedies to address and rectify the illegal conduct and actions described herein, to enjoin Defendant from making similar disclosure of its patients' Private Information in the future, and to fully articulate, *inter alia*, the specific Private Information it disclosed to third parties and to identify the recipients of that information.

29. Defendant breached its statutory and common law obligations to Plaintiffs and Class Members by, *inter alia*,: (i) installing and configuring, and then failing to remove or disengage, technology that was known and designed to share web-users' information; (ii) failing to obtain the written consent of Plaintiffs and Class Members to disclose their Private Information to Facebook or others; (iii) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through Tracking Technologies like the Meta Pixel, Google Analytics, Google DoubleClick, or LinkedIn Insight Tag; (iv) failing to warn Plaintiffs and Class Members; and (v) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

30. As a result of Defendant's conduct, Plaintiffs and Class Members have suffered numerous injuries including, but not limited to: (i) invasion of privacy; (ii) loss of benefit of the

[13] CityMD breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web-based technology to ensure the Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share patients' Private Information; (iii) failing to obtain the consent of patients, including Plaintiffs and Class Members, to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through the Pixels and Conversions API; (v) failing to warn Plaintiffs and Class Members of such sharing and disclosures; and (vi) otherwise failing to design and monitor the Website to maintain the confidentiality and integrity of patients' Private Information.

bargain; (iii) diminution of value of their Private Information; (iv) statutory damages; and (v) the continued and ongoing risk to their Private Information.

31. Plaintiffs seek to remedy these harms and brings causes of action for (i) violation of the Electronics Communication Privacy Act ("ECPA"), 18 U.S.C. § 2511(1), *et seq.*; (ii) breach of implied contract; (iii) negligence; (iv) breach of confidence; (v) constructive bailment; (vi) violation of the New York Deceptive Trade Practices Act, New York Gen. Bus. Law § 349, *et seq.*; (vii) invasion of privacy; and (viii) unjust enrichment.

PARTIES

32. Plaintiff V.A. is, and at all relevant times was, an individual residing in New York County, in the State of New York.

33. Plaintiff T.G. is, and at all relevant times was, an individual residing in Suffolk County, in the State of New York.

34. Defendant Summit Health Management LLC is a domestic corporation incorporated in the State of New Jersey. Defendant is a covered entity under HIPAA.

JURISDICTION & VENUE

35. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because this Complaint asserts a claim for violation of federal law, the ECPA, 18 U.S.C. § 2511. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

36. This Court also has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this case is brought as a class action where the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in

the proposed class, and one or more putative Class members including Plaintiffs are citizens of a different state than Defendant.

37. This Court has personal jurisdiction over Summit Health because Defendant Summit Health Management LLC is located in the state of New Jersey – specifically, in this District, the parties are citizens of different states and the amount in controversy exceeds $75,000, 28 U.S.C. § 1332(a)(1). Additionally, this Court has personal jurisdiction over Defendant because Summit Health is authorized to and regularly conducts business in this judicial district.

38. Venue is proper under 28 U.S.C § 1391(b)(2) Defendant's principal place of business is in this district, Defendant conducts business in this district, and a substantial part of the events, acts and omissions which gave rise to these claims occurred in this district.

COMMON FACTUAL ALLEGATIONS

A. Federal Regulators Make Clear that the Use of Tracking Technologies to Collect & Divulge Private Information Without Informed Consent is Illegal

39. This surreptitious collection and divulgence of Private Information is an extremely serious data security and privacy issue. Both the Federal Trade Commission and the Office for Civil Rights ("OCR") of the Department of Health and Human Services ("HHS") have, in recent months, reiterated the importance of and necessity for data security and privacy concerning health information.

40. For instance, the FTC recently published a bulletin entitled *Protecting the privacy of health information: A baker's dozen takeaways from FTC cases*, in which it noted that "[h]ealth information is not just about medications, procedures, and diagnoses. ***Rather, it is anything that conveys information—or enables an inference—about a consumer's health***. Indeed, [recent FTC enforcement actions involving] *Premom*, *BetterHelp*, *GoodRx* and *Flo Health* ***make clear that the fact that a consumer is using a particular health-related app or website—one related to***

mental health or fertility, for example—or how they interact with that app (say, turning 'pregnancy mode' on or off) may itself be health information."[14]

41. The FTC is unequivocal in its stance as it informs—in no uncertain terms—healthcare companies that they should ***not*** use tracking technologies to collect sensitive health information and disclose it to various platforms without informed consent:

> **Don't use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.**
>
> In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. ***But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.***
>
> [Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that ***may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information***.[15]

42. The federal government is taking these violations of health data privacy and security seriously as recent high-profile FTC settlements against several telehealth companies evidence. For example, earlier this year, the FTC imposed a $1.5 million penalty on GoodRx for violating the FTC Act by sharing its customers' sensitive PHI with advertising companies and

[14] *See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases,* FTC Business Blog (July 25, 2023) (emphasis added), https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases.

[15] *Id.* (emphasis added) (further noting that *GoodRx* & *Premom* underscore that this conduct may also violate the Health Breach Notification Rule, which requires notification to consumers, the FTC and, in some cases, the media, of disclosures of health information without consumers' authorization.

platforms, including Facebook, Google and Criteo, and a $7.8 million settlement with the online counseling service BetterHelp, resolving allegations that the company shared customer health data with Facebook and Snapchat for advertising purposes. And Easy Healthcare was ordered to pay a $100,000 civil penalty for violating the Health Breach Notification Rule when its ovulation tracking app Premon shared health data for advertising purposes.[16]

43. Even more recently, in July 2023, federal regulators sent a letter to approximately 130 healthcare providers warning them about using online tracking technologies that could result in unauthorized disclosures of Private Information to third parties. The letter highlighted the "risks and concerns about the use of technologies, such as the Meta/Facebook Pixel and Google Analytics, that can track a user's online activities," and warned about "[i]mpermissible disclosures of an individual's personal health information to third parties" that could "result in a wide range of harms to an individual or others." According to the letter, "[s]uch disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more."[17]

---

[16] *See How FTC Enforcement Actions Will Impact Telehealth Data Privacy*, Health IT Security, https://healthitsecurity.com/features/how-ftc-enforcement-actions-will-impact-telehealth-data-privacy (last visited Jun. 14, 2024); *See* Allison Grande, *FTC Targets GoodRx In 1st Action Under Health Breach Rule*, Law360 (Feb. 1, 2023), www.law360.com/articles/1571369/ftc-targets-goodrx-in1st-action-under-health-breach-rule?copied=1 ("The Federal Trade Commission signaled it won't hesitate to wield its full range of enforcement powers when it dinged GoodRx for allegedly sharing sensitive health data with advertisers, teeing up a big year for the agency and boosting efforts to regulate data privacy on a larger scale."); https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising; https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc (last visited Jan. 14, 2025).

[17] Office for Civil Rights, *Use of Online Tracking Technologies* (July 20, 2023), , https://www.hhs.gov/sites/default/files/use-online-tracking-technologies.pdf (last visited Jan. 15,

44. Moreover, the Office for Civil Rights at HHS has made clear, in a recent bulletin titled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the transmission of such protected information violates HIPAA's Privacy Rule:

> **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.[18]

45. The OCR Bulletin discusses the harms that disclosure may cause patients:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss,

---

2025).

[18] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, Dept. of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (noting that "IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as in some circumstances IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.").

On June 20, 2024, this guidance was vacated *in part* by Judge Pittman of in the Northern District of Texas due to the court finding it in part to be the product of improper rulemaking and it is cited for reference only until the OCR updates its guidance, should it do so in the future. *See Am. Hosp. Ass'n. v. Becerra*, No. 4:23-cv-01110-P, ECF No. 67 (S.D. Tex., June 20, 2024). Notably, the court's order found *only* that the OCR's guidance regarding covered entities disclosing to third parties users' IP addresses while those users navigated *unauthenticated public webpages* ("UPWs") was improper rulemaking. The Order in no way affects or undermines the OCR's guidance regarding covered entities disclosing personal identifiers, such as Google or Facebook identifiers, to third parties while patients were making appointments for particular conditions, paying medical bills or logging into (or using) a patient portal. *See id*. at 3-4, 31, n. 8 (vacating the OCR guidance with respect to the "Proscribed Combination" defined as "circumstances where an online technology connects (1) an individual's IP address with (2) a visit to a UPW addressing specific health conditions or healthcare providers" but stating that "[s]uch vacatur is not intended to, and should not be construed as, limiting the legal operability of other guidance in the germane HHS document."). The FTC bulletin on the same topics remains untouched as do the FTC's enforcement actions against healthcare providers for committing the same actions alleged herein.

> ***discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI.*** Such disclosures can reveal incredibly sensitive information about an individual, ***including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.*** While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.***[19]

46. Investigative journalists have published several reports detailing the seemingly ubiquitous use of tracking technologies on hospitals', health care providers' and telehealth companies' digital properties to monetize their Users' Private Information.

47. For instance, THE MARKUP reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment.[20]

48. And, in the aptly titled report *"Out of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, a joint investigation by STAT and THE MARKUP of 50 direct-to-consumer telehealth companies reported that telehealth companies or virtual care websites were providing sensitive medical information they collect to the world's largest advertising platforms.[21]

---

[19] *Id.* (emphasis added).

[20] *See* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

[21] Todd Feathers, Katie Palmer (STAT) & Simon Fondrie-Teitler, *"Out Of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies: An investigation by The Markup and STAT found 49 out of 50 telehealth websites sharing health data via Big Tech's*

49. Many telehealth sites had at least one tracker—from Meta, Google, TikTok, Bing, Snap, Twitter, LinkedIn and/or Pinterest—that collected patients' answers to medical intake questions.[22]

50. In the case of CityMD, it appears to have installed at least the following tracking pixels, cookies and other invisible codes from the following data brokers: Facebook, Google, LinkedIn, Bing, Blue Cava, Magnite, and Pubmatic.

B. Summit Health Installed Facebook, Google and LinkedIn Trackers to Collect Patients' PII and PHI on the CityMD Website

a. *Facebook Tracking Tools*

51. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[23]

52. Facebook describes itself as a "real identity platform,"[24] meaning users are allowed only one account and must share "the name they go by in everyday life."[25] To that end, when

tracking tools, The Markup (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies

[22] *See id.* (noting that "[t]rackers on 25 sites, including those run by industry leaders Hims & Hers, Ro, and Thirty Madison, told at least one big tech platform that the user had added an item like a prescription medication to their cart, or checked out with a subscription for a treatment plan").

[23] *Facebook, Meta Reports Fourth Quarter and Full Year 2021 Results*, FACEBOOK, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Jan. 12, 2025).

[24] Sam Schechner & Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL ST. J. (Oct. 21, 2021, 4:05 PM), https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701.

[25] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.

creating an account, users must provide their first and last name, along with their birthday and gender.[26]

53. Facebook sells advertising space by highlighting its ability to target users.[27] Facebook can target users effectively because it surveils user activity on and off its site.[28] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[29] Facebook compiles this information into a generalized dataset called "Core Audiences," which allows advertisers to reach precise audiences based on specified targeting types.[30]

54. Advertisers can also build "Custom Audiences."[31] Custom Audiences enables advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[32] With Custom Audiences, advertisers can target existing customers directly and build "Lookalike Audiences," which "leverage[] information such as demographics, interests and behaviors from your source

[26] FACEBOOK, SIGN UP, https://www.facebook.com.

[27] FACEBOOK, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, https://www.facebook.com/business/help/205029060038706.

[28] FACEBOOK, ABOUT META PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

[29] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

[30] FACEBOOK, https://www.facebook.com/business/news/Core-Audiences.

[31] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494.

[32] FACEBOOK, AUDIENCE AD TARGETING, https://www.facebook.com/business/ads/ad-targeting.

audience to find new people who share similar qualities."[33] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: (1) by manually uploading contact information for customers or (2) by utilizing Facebook's "Business Tools."[34]

55. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendant, to utilizes its "Business Tools" to gather, identify, target, and market products and services to individuals.

56. Facebook's Business Tools, including the Meta Pixel ("Pixel") and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications and servers, thereby enabling the interception and collection of website visitors' activity.

57. Specifically, the Pixel "tracks the people and type of actions they take."[35] When a user accesses a webpage hosting the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook's servers. Notably, this transmission does not occur unless the webpage contains the Pixel.

58. Facebook's own documentation makes clear how extensively the Facebook Tracking Pixel tracks private information. It describes the Facebook Tracking Pixel as code that Facebook's business customers can put on their website to "[m]ake sure your ads are shown to the

---

[33] FACEBOOK, ABOUT LOOKALIKE AUDIENCES, https://www.facebook.com/business/help/164749007013531?id=401668390442328.

[34] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; FACEBOOK, CREATE A WEBSITE CUSTOM AUDIENCE, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494.

[35] RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Jan. 12, 2025).

right people[] [and] ***[f]ind . . . people who have visited a specific page or taken a desired action on your website***" (emphasis added).[36]

59. The Pixel is customizable and programmable, meaning that the website owner controls which of its web pages contain the Pixel and which events are tracked and transmitted to Facebook.

60. The process of adding the Pixel to webpages is a multi-step process that must be undertaken by the website owner.[37]

61. Facebook guides the website owner through setting up the Pixel during the setup process. Specifically, Facebook explains that there are two steps to set up a pixel: "(1) Create your pixel and set up the pixel base code on your website. You can use a partner integration if one is available to you or you can manually add code to your website. (2) Set up events on your website to measure the actions you care about, like making a purchase. You can use a partner integration, the point-and-click event setup tool, or you can manually add code to your website."[38]

62. Aside from the various steps to embed and activate the Pixel, website owners, like Defendant, must also agree to Facebook's Business Tools Terms by which Facebook requires website owners using the Pixel to "represent and warrant" that they have adequately and prominently notified users about the collection, sharing and usage of data through Facebook's Business Tools (including the Pixel) and that websites "will not share Business Tool Data . . . that

---

[36] META, ABOUT META PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

[37] Business Help Center: How to set up and install a Meta Pixel, https://www.facebook.com/business/help/952192354843755?id=1205376682832142 (last visited Jan. 12, 2025).

[38] *Id.*

[websites] know or reasonably should know . . . includes health, financial information or other categories of sensitive information . . . ."[39]

63. Stated differently, Plaintiffs' and Class Members' Private Information would not have been disclosed to Facebook but for the Defendant's decision to install Facebook tracking technologies on its Website.

64. As explained in more detail below, this secret transmission to Facebook is initiated by Defendant's source code concurrently with Plaintiffs' and Class Members' communications to their intended recipient, Defendant.

b. *Google Tracking Tools*

65. Alphabet Inc., the parent holding company of Google, generates revenues primarily by delivering targeted online advertising through Google, which is the creator of the Google Source Code and an established advertising company.

66. Google Source Code—the source code associated with Google's advertising system and products, including Google Analytics—is designed to track and collect individuals' information when they are browsing the internet.

67. Google Source Code is provided by Google in a copy-and-paste format, and its functionality is uniform on all web properties, with the option for website operators like CityMD to choose to disclose additional data about its users to Google. Its operation is hidden by Google's design and does not indicate to users that Google Source Code is present on a website they are visiting.

[39] *Id.*; *see also* Pratyush Deep Kotoky, *Facebook collects personal data on abortion seekers: Report* (June 16, 2022), https://www.newsbytesapp.com/news/science/facebook-collects-personaldata-on-abortion-seekers/story (quoting Facebook spokesman Dale Hogan as saying that it is "against [Facebook's] policies for websites and apps to send sensitive health data about people through [its] Business Tools") (last visited Jan. 12, 2025).

68. When the Google Source Code is placed by website operators such as CityMD on their website, CityMD's actions allow the Google Source Code to instruct the computer accessing CityMD's web pages to track, intercept, and redirect the user's information to Google.

69. This tracking, interception, and redirection of information occurs when individuals exchange communications or requests with the relevant web pages.

70. Google Analytics, a marketing tool used for advertising and analytics, is one of Google's primary products and services that leverage Google Source Code to track, collect, and subsequently use (i.e., monetize) individuals' personal information. A fundamental and primary purpose of Google Analytics is to obtain information about consumers' communications and activities that is accessible by entities other than Google. Google accomplishes this through Google Analytics, in part, by touting it as a tool that enables clients to "understand the customer journey and improve marketing ROI."[40] Specifically, according to Google, Google Analytics is intended to help advertisers:

a. "Unlock customer-centric measurement" to "[u]nderstand how your customers interact across your sites and apps, throughout their entire lifecycle;"

b. "Get smarter insights to improve ROI," to "[u]ncover new insights and anticipate future customer actions with Google's machine learning to get more value out of your data;" and

c. "Connect your insights to results," to "[t]ake action to optimize marketing performance with integrations across Google's advertising and publisher tools[.]"[41]

71. Like the Meta Pixel, when a user exchanges information with the host of a website—such as through a search query—Google Source Code operates to surreptitiously direct the user's browser to send a separate message to Google's servers. This second, secret transmission

[40] Google Marketing Platform, *Analytics*, https://marketingplatform.google.com /about/analytics/.

[41] *Id.*

contains the original request sent to the host website, ("GET request"), along with additional data that the Google Source Code is configured to collect ("POST request"). These transmissions are initiated by Google Source Code and concurrent with the communications to and from the host website.

72. Google Analytics offers website developers like CityMD the option to include additional data of their own choosing about its users' activities in any communications to Google, including "Event Value" and "Event Label" data. As can be seen from the Google Analytics developer website, this data is optional and not sent to Google by default.[42]

73. Upon information and good faith belief, Defendant enabled such additional data collection from its patients, and also chose to disclose search terms users entered into the Website search bar to Google via Google Analytics by enabling the Google Analytics "enhanced event measurement" feature.

74. In other words, CityMD took affirmative, additional steps of its own to configure Google Analytics' tracking's ability to ensure that Google received additional data about its website users.

75. Also like the Meta Pixel, Google associates the information it obtains via Google Source Code with other information regarding the user, using personal identifiers that are transmitted concurrently with other information the code is configured to collect. These identifiers include the "cid," a combination of the time at which the user visited the website and a unique identifier. The "cid" is assigned to an individual's browser and can persist for up to two years, allowing Google to link a series of events to the same browser and, thus, to an individual. For Google account holders, this identifier is also linked to that account.

[42] *See* Google Analytics, *Measurement Protocol Parameter Reference*, https://developers.google.com/analytics/devguides/collection/protocol/v1/parameters.

76. Google also uses DoubleClick cookies including DSID and IDE that operate similarly to the unique Facebook ID, to track unique users across websites and target them with ads based on their browsing activities.

77. In addition to information gleaned from a user's unique ID, Google can create a unique, digital "fingerprint" for a user based on data transmitted via Google Source Code, which allows Google to link certain web activity to a user. This "fingerprint" can consist of information regarding a user's screen depth, screen resolution, browser name and version, and operating system name and version, as well as a user's Internet Protocol ("IP") address. With that information, Google is able to link data acquired through Google Analytics to a particular user.[43]

78. Browser-fingerprints are also considered personal identifiers, and tracking pixels can collect browser-fingerprints from website visitors. Browser-fingerprints are protected personal identifiers under HIPAA. *See* 45 C.F.R. § 164.514(b)(2)(i)(M), (R).

79. After tracking, intercepting, and acquiring user's information, Google uses the information for personalized advertising in its advertising systems which includes, but is not limited to, Google Analytics.

80. For example, Google Analytics uses the information it collects to facilitate its Audience Targeting feature. Audience Targeting refers to serving ads to only a select number of users who share certain common characteristics. For Google's Audience Targeting, Google can target ads to either "Pre-defined Google Audiences" or "Advertiser-curated Audiences." Pre-defined Audiences are those created by Google based on interest and demographic data.

[43] In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users. *See* https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/.

Advertiser-curated Audiences are customized audiences created by Google through the use of the Source Code, including audiences created through Google Analytics.

81. Like Meta, Google is therefore able to monetize the information surreptitiously intercepted, with CityMD's help, from visitors to the CityMD Site.

c. *LinkedIn Tracking Tools*

82. LinkedIn develops, owns and operates "the world's largest professional network with more than 1 billion members in more than 200 countries and territories worldwide."[44]

83. LinkedIn is also an advertising company that touts its ability to deliver targeted marketing to specific users.

84. It does so by using its proprietary software, including the tracker known as the LinkedIn Insight Tag.

85. The LinkedIn Insight Tag is a snippet of JavaScript code that allows website owners "to track LinkedIn ad-driven visitor activity on your website. It relies on LinkedIn cookies, which enable [LinkedIn] to match your website visitors to their respective LinkedIn member accounts."[45]

86. According to LinkedIn, "[t]argeting is a foundational element of running a successful advertising campaign — [g]etting your targeting right leads to higher engagement, and ultimately, higher conversion rates."[46]

87. Targeting refers to ensuring that advertisements are targeted to, and appear in front of, the target demographic for an advertisement. To that end, LinkedIn's Marketing Solutions

---

[44] *About*, https://about.linkedin.com/?trk=homepage-basic_directory_aboutUrl.

[45] *Insight Tag*, https://business.linkedin.com/marketing-solutions/insight-tag.

[46] *Reach your audience: Targeting on LinkedIn*, p.3, https://business.linkedin.com/content/dam/me/business/en-us/marketingsolutions/resources/pdfs/linkedin-targeting-playbook-v3.pdf.

services allow potential advertisers to "[b]uild strategic campaigns" targeting specific users.[47] LinkedIn's "marketing solutions allow advertisers to select specific characteristics to help them reach their ideal audience. The ads [users] see on LinkedIn are then targeted to provide content relevant to [the users]."[48]

88. The personal information, communications, and other user data obtained by LinkedIn are used to fuel various services offered via LinkedIn's Marketing Solutions including Ad Targeting, Matched Audiences, Audience Expansion, and LinkedIn Audience Network.[49]

89. Such data is extremely valuable because the inferences derived from users' personal information and communications allow marketers and advertisers, including healthcare providers and insurance companies, to target potential customers based on their personal traits and by their professional or personal interests.[50]

90. LinkedIn represents that the LinkedIn Insight Tag "enable[s] in-depth campaign reporting and unlock[s] valuable insights about your website visitors."[51]

91. A critical feature allows the LinkedIn Insight Tag to track users even when third-party cookies are blocked. In fact, LinkedIn "recommend[s] using the JavaScript-based Insight Tag or Conversions API" because third-party cookie settings are being deprecated across the industry."[52]

---

[47] *Marketing Solutions*, https://business.linkedin.com/marketing-solutions.

[48] *LinkedIn Ads and Marketing Solutions*, https://www.linkedin.com/help/lms/answer/a421454.

[49] *Marketing Solutions*, https://business.linkedin.com/marketingsolutions/Audience.

[50] *See Account Targeting*, https://business.linkedin.com/marketing-solutions/ad-targeting.

[51] *LinkedIn Insight Tag FAQs*, https://www.linkedin.com/help/lms/answer/a427660.

[52] *Insight Tag*, https://business.linkedin.com/marketing-solutions/insight-tag.

92. Embedding the JavaScript as a first-party cookie causes users' browsers to treat the LinkedIn Insight Tag as though it is offered by the website being visited, rather than by LinkedIn. Doing so ensures that the third-party cookie-blocking functions of modern web browsers do not prevent LinkedIn from collecting data through its software. Instead, the LinkedIn Insight Tag is shielded with the same privacy exemptions offered to first-party cookies.[53]

93. When a user who has signed in to LinkedIn (even if the user subsequently logs out) is browsing a website where the LinkedIn Insight Tag has been embedded, an HTTP request is sent using cookies, which includes information about the user's actions on the website.

94. These cookies also include data–collected via LinkedIn cookies – that differentiates users from one another and can be used to link the information collected to the user's LinkedIn profile.

95. These cookies also include data that differentiates users from one another and can be used to link the data collected to the user's LinkedIn profile.

96. Specifically, LinkedIn utilizes the "li_sugr" cookie "to make a probabilistic match of a user's identity."[54] Similarly, LinkedIn uses the "lms_ads" cookie "to identify LinkedIn Members off LinkedIn for advertising."[55]

97. A person's LinkedIn profile contains information including an individual's first and last name, place of work, contact information, and other personal details. Based on information it obtains through the LinkedIn Insight Tag, LinkedIn is then able to target its account holders for advertising.

---

[53] *See id.*

[54] *See id*.

[55] *See id*.

98. Accordingly, just like Facebook and Google, LinkedIn also monetizes the Private Information of CityMD's patients that it receives from CityMD's Website.

C. CityMD Assisted Unauthorized Third Parties in Intercepting Patients' Communications with its Website and Disclosed Their Private Information to Third Parties.

99. Defendant's Website is accessible on mobile devices and desktop computers and allows patients to communicate with Defendant regarding their PHI, medical care and bill payment.

100. Defendant encouraged patients to use its Website to communicate their Private Information, schedule appointments, access information about their treatments, pay medical bills and more.

101. Despite this, Defendant purposely installed Tracking Technologies including, but not limited to, the Meta Pixel, Google Analytics, Google DoubleClick, and the LinkedIn Insight Tag on its Website and programmed specific webpage(s) to surreptitiously share its patients' private and protected communications, including Plaintiffs' and Class Members' PHI and/or PII, which was sent to Facebook, Google, LinkedIn and other third parties.

102. The Tracking Technologies followed, recorded and disseminated patients' information as they navigated and communicated with Defendant via the Website, simultaneously transmitting the substance of those communications to unintended and undisclosed third parties.

103. The information disseminated by the Tracking Technologies and/or intercepted by third parties constitutes Private Information including medical information patients requested or viewed, the title of any buttons clicked (such as the "Women's Health" dropdown button under "Services," which indicates the patient has signaled a desire for treatment specifically for women's health issues), the exact phrases typed into text boxes, other selections made from drop-down

menus or while using other sensitive and confidential information, the divulgence of which is and was highly offensive to Plaintiffs and Class Members.

104. As described by the OCR Bulletin, this is PHI because the webpages have access to "information that relates to any individual's past, present, or future health, health care, or payment for health care."[56]

105. The information collected and disclosed by Defendant's Tracking Technologies is not anonymous and is viewed and categorized by the intercepting party upon receipt.

106. The information Facebook received via the Meta Pixel was linked and connected to patients' Facebook profiles (via their Facebook ID or "c_user id"), which includes other PII.

107. Similarly, through its Tracking Technologies, Google stores users' logged-in identifiers on non-Google websites in its logs. Whenever a user logs-in on non-Google websites, whether in private browsing mode or non-private browsing mode, the same identifier is associated with the data Google collects from the user's browsing activities on that website. Google further logs all such data (private and non-private) within the same logs and uses these data for serving personalized ads.

108. And as described above, LinkedIn utilizes its Insight Tag and LinkedIn cookies to collect and connect CityMD's patients' Private Information to their personal LinkedIn accounts.

109. The health information that was disclosed via the Tracking Technologies is personally identifiable and was sent alongside other persistent unique identifiers such as the patients' IP address, their unique Facebook, Google, and LinkedIn IDs, and device identifiers.[57]

---

[56] *See* OCR Bulletin *supra, note 19*.

[57] *See Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1056 (N.D. Cal. 2021) (discussing how Google collects personal information and IP addresses); *see also* https://developers.facebook.com/docs/meta-pixel/ (last visited Jan. 12, 2025).

D. Underlying Web Technology.

110. Web browsers are software applications that allow consumers to navigate the internet and exchange electronic communications, and every "client device" (computer, tablet or smart phone) has a web browser (*e.g.*, Microsoft Edge, Google Chrome, Mozilla's Firefox, etc.).

111. When patients used Defendant's Website, they engaged in an ongoing back-and-forth exchange of electronic communications with Defendant wherein their web browser communicated with Defendant's computer server—like how two telephones communicate.

112. These communications are invisible to ordinary consumers,[58] but one browsing session may consist of thousands of individual HTTP Requests and HTTP Responses.

113. A patient's HTTP Request essentially asks the Defendant's Website to retrieve certain information (such as a "Find a CityMD" webpage), and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons and other features that appear on the patient's screen as they navigate Defendant's Website).

114. Every webpage is comprised of both Markup and "source code." Source code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

115. Defendant's Tracking Technologies were embedded in its Website' source code, which is contained in its HTTP Response. The Tracking Technologies, which were programmed to automatically track patients' communications and transmit them to third parties, executed instructions that effectively opened a hidden spying window into each patients' web browser, through which third parties intercepted patients' communications and activity.

[58] *See* OCR Bulletin *supra,* note 19 ("Tracking technologies collect information and track users in various ways, many of which are not apparent to the website or mobile app user.").

116. For example, when a patient visits www.citymd.com and selects the "Virtual Care" or "Get Care Now" button, the patient's browser automatically sends an HTTP Request to Defendant's web server. Defendant's web server automatically returns an HTTP Response, which loads the Markup for that particular webpage. The user only sees the Markup, not Defendant's source code or underlying HTTP Requests and Responses.

117. Behind the scenes, however, Tracking Technologies like the Meta Pixel, Google Analytics, and LinkedIn trackers are embedded in the source code, automatically transmitting everything the patient does on the webpage and effectively opening a hidden spy window into the patient's browser.

118. These transmissions occur contemporaneously, invisibly and without the patient's knowledge and consent.

119. The Tracking Technologies allow Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences and decrease advertising and marketing costs. However, Defendant's Website does not rely on the Tracking Technologies to function.

120. Plaintiffs and Class Members never consented, agreed, authorized or otherwise permitted Defendant to disclose their Private Information to third parties, nor did they intend for anyone other than Defendant to be a party to their communications (many of them highly sensitive and confidential) with Defendant.

121. Defendant's Tracking Technologies sent non-public Private Information to third parties like Facebook, Google and LinkedIn, including but not limited to Plaintiffs' and Class Members': (i) status as medical patients; (ii) health conditions; (iii) medical treatments; (iv) locations where treatment was sought; (v) bill payment and/or insurance coverage information;

and (vi) search queries, such as searches for medical treatment options and medical information specific to patients' medical conditions.

122. Importantly, the Private Information that Defendant's Tracking Technologies sent to third parties included PII such as patients' unique personal identifiers that allowed those third parties to connect the Private Information to a specific patient.

123. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (i) implemented Tracking Technologies that surreptitiously tracked, recorded and disclosed Plaintiffs' and other patients' confidential communications and Private Information; (ii) disclosed patients' protected information to unauthorized third parties; and (iii) undertook this pattern of conduct without notifying Plaintiffs or Class Members and without obtaining their express written consent.

E. Defendant's Tracking Technologies Disseminate Patient Information Via Its Website.

124. If a patient uses Defendant's Website to find care, the Website directs them to communicate Private Information, including but not limited to the reason (i.e. the medical condition and/or symptoms) for seeking care, exact search terms entered into the search bar, type of visit (office or virtual), specific location of their visit, and their status as medical patients.

125. Unbeknownst to the patient, these communications are sent to Facebook and other third-party entities via Defendant's Tracking Technologies.

126. For example, Defendant's Website offers patients the option of selecting various types of specific services, including from such categories as "injuries," "illnesses," "on-the-job injuries," "women's health," and "occupational medicine."[59]

[59] *See* https://www.citymd.com/services (last visited Jan. 14, 2025).

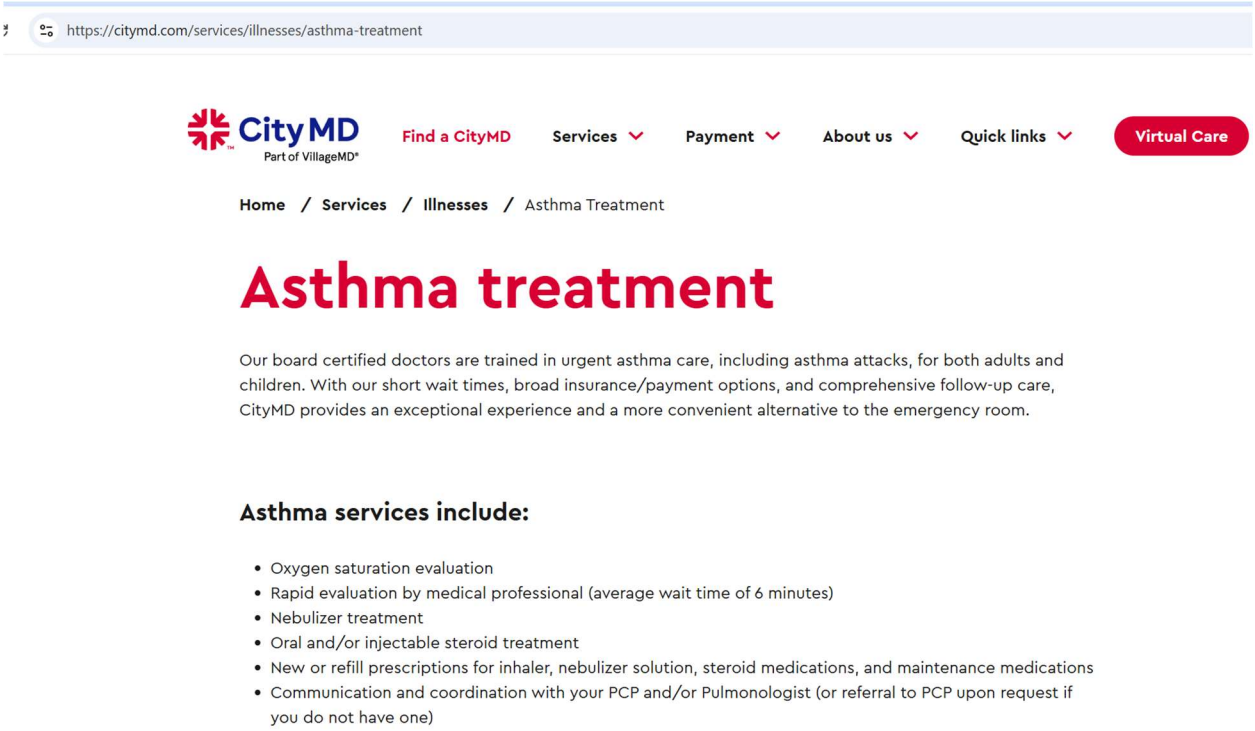
127. In some categories of services offered by Defendant, a User can select even more specific conditions, such as:

a. "UTI testing,"

b. "asthma treatment," or

c. "COVID-19."[60]

Figure 1: Screenshot from the CityMD Website depicting a webpage as seen by patients:



128. Defendant discloses these searches and selections by its patients and/or prospective patients to Facebook (and other unauthorized third parties), as illustrated in the examples below which show the "behind the scenes" portion of the website that is invisible to ordinary users.

Figures 2-4. Examples of Users' searches for and selections of CityMD's services related to their specific medical conditions along with the User's unique personal identifier from Facebook, the c_user cookie:

60 *See* https://www.citymd.com/services/womens-health/uti-testing; https://www.citymd.com/services/illnesses (last visited Jan. 14, 2025).

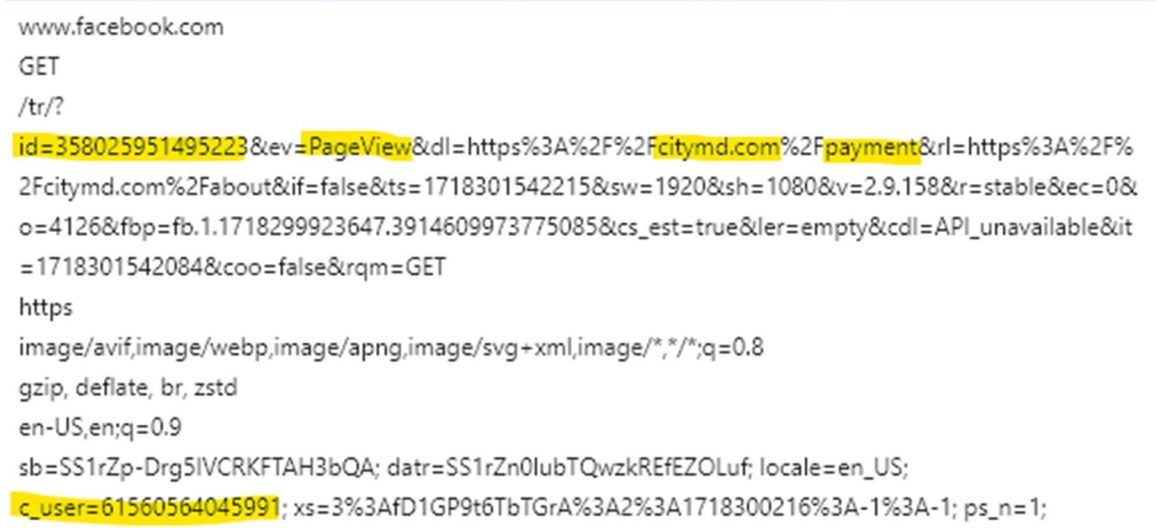
www.facebook.com
GET
/tr/?id=358025951495223&ev=PageView&dl=https%3A%2F%2Fcitymd.com%2Foccupational-medicine%2Fwork-related-injury-care&rl=https%3A%2F%2Fcitymd.com%2Foccupational-medicine&if=false&ts=1718301854668&sw=1920&sh=1080&v=2.9.158&r=stable&ec=0&o=4126&fbp=fb.1.1718299923647.3914609973775085&cs_est=true&ler=empty&cdl=API_unavailable&it=1718301854637&coo=false&rqm=GET
https
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
gzip, deflate, br, zstd
en-US,en;q=0.9
sb=SS1rZp-Drg5IVCRKFTAH3bQA; datr=SS1rZn0lubTQwzkREfEZOLuf; locale=en_US; c_user=61560564045991;

www.facebook.com
GET
/tr/?id=358025951495223&ev=PageView&dl=https%3A%2F%2Fcitymd.com%2Fservices%2Fillnesses%2Fasthma-treatment&rl=https%3A%2F%2Fcitymd.com%2Fservices%2Fillnesses&if=false&ts=1718301953610&sw=1920&sh=1080&v=2.9.158&r=stable&ec=0&o=4126&fbp=fb.1.1718299923647.3914609973775085&cs_est=true&ler=empty&cdl=API_unavailable&it=1718301953460&coo=false&rqm=GET
https
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
gzip, deflate, br, zstd
en-US,en;q=0.9
sb=SS1rZp-Drg5IVCRKFTAH3bQA; datr=SS1rZn0lubTQwzkREfEZOLuf; locale=en_US; c_user=61560564045991;

www.facebook.com
GET
/tr/?id=358025951495223&ev=PageView&dl=https%3A%2F%2Fcitymd.com%2Fservices%2Fwomens-health%2Futi-testing&rl=https%3A%2F%2Fcitymd.com%2Fservices%2Fwomens-health&if=false&ts=1718301149913&sw=1920&sh=1080&v=2.9.158&r=stable&ec=0&o=4126&fbp=fb.1.1718299923647.3914609973775085&cs_est=true&ler=empty&cdl=API_unavailable&it=1718301149857&coo=false&rqm=GET
https
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
gzip, deflate, br, zstd
en-US,en;q=0.9
sb=SS1rZp-Drg5IVCRKFTAH3bQA; datr=SS1rZn0lubTQwzkREfEZOLuf; locale=en_US; c_user=61560564045991;
xs=3%3AfD1GP9t6TbTGrA%3A2%3A1718300216%3A-1%3A-1; ps_n=1;
fr=0vbOhFaz3aPbghfXm.AWVv52GBpAC5neUol2tqgtMX4uk.Bmay1J..AAA.0.0.BmazCe.AWXJKQvOvLc
i
https://citymd.com/

129. Defendant also discloses when a User makes a payment for CityMD's services:

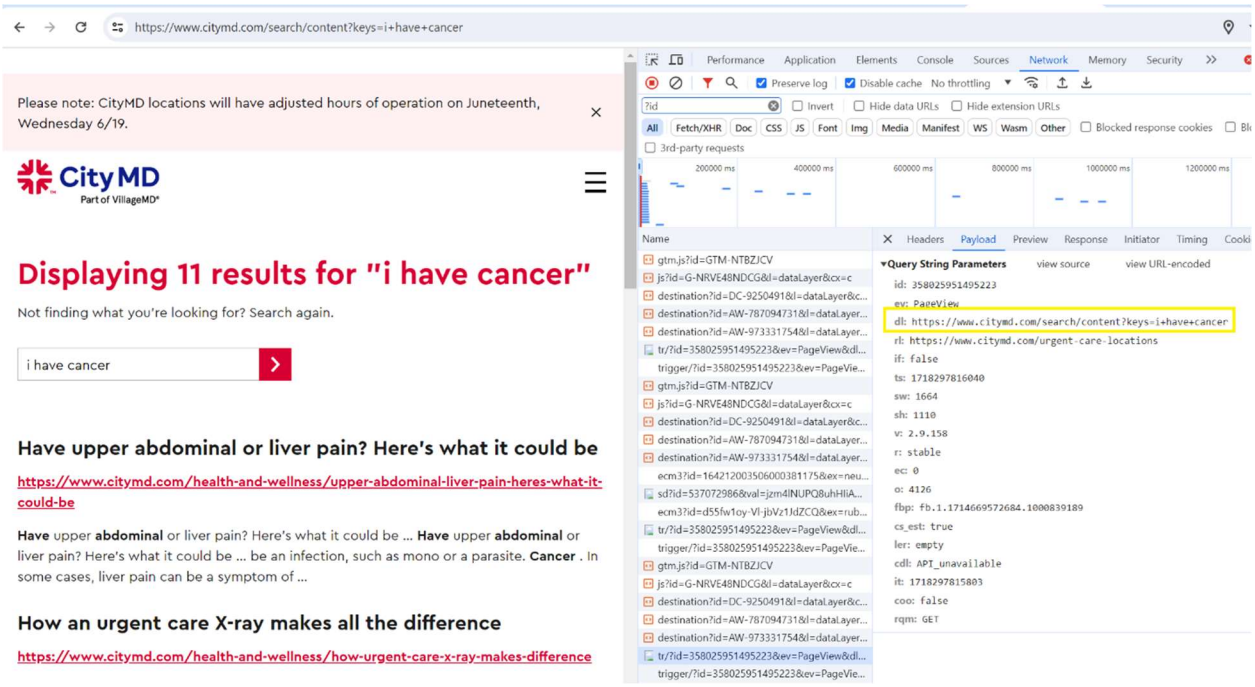
Figure 5. Defendant's disclosure of a User's Private Information, including patient status and personal identifiers, when they review their payment options on the Website.



130. To make matters worse, Defendant's Tracking Technologies even track and record the exact text and phrases that a user types into the general search bar located on Defendant's homepage. In the example below, the user typed "I have cancer" into the search bar.

131. That exact phrase is sent to Facebook, thereby allowing the user's medical condition to be linked to their individual Facebook account for future retargeting and exploitation. There is no legitimate reason for sending this information to Facebook.

Figure 6. Example of the disclosure of the user's exact search terms "I have cancer" from the Website search bar to Facebook.



132. In each of the examples above, the user's website activity and the contents of their communications are sent to Facebook alongside their PII. Marketers and other third parties are able to personally identify individual website users through several means, but the examples above demonstrate what happens when the website user is logged into Facebook on their web browser or device. When this happens, the website user's identity is revealed via third-party cookies that work in conjunction with the Tracking Technologies.

133. For example, Facebook receives at least seven cookies when Defendant's Website transmits information via the Meta Pixel, including the user's c_user cookie which contains the user's unencrypted Facebook ID, and allows Facebook to link the user's online communications and interactions to their individual Facebook profile:

Figure 7. Screenshot of network analysis showing cookies sent to Facebook when a user visits CityMD.com.

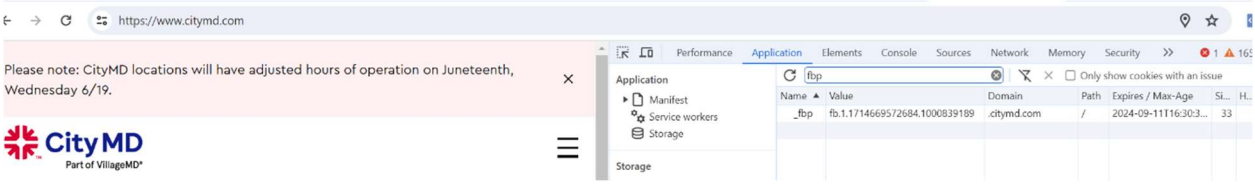
Name	Value	Domain
c_user	540643061	.facebook.com
datr	Y5QdZurO628alqBjNG42Gs_R	.facebook.com
fr	1OESf4gzhe953FZd9.AWUI0wArTMYW6m...	.facebook.com
ps_l	1	.facebook.com
ps_n	1	.facebook.com
sb	GrxtY1jj9lKWnpCg7UAhiJMv	.facebook.com
xs	7%3Ag2wyjfuNYXsJFg%3A2%3A1707506...	.facebook.com

134. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies, including the fr and datr cookies.

135. The fr cookie contains an encrypted Facebook ID and browser identifier.[61] Facebook, at a minimum, uses the fr cookie to identify users, and this cookie can stay on a user's website browser for up to 90 days after the user has logged out of Facebook.[62]

136. At each stage, Defendant also utilizes the _fbp cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user. [63]

Figure 8. Screenshot showing Defendant's use of first party _fbp cookie.



[61] Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit* (Sept. 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited Jan. 14, 2025).

[62] *Cookies & other storage technologies*, https://www.facebook.com/policy/cookies/ (last visited Jan. 14, 2025).

[63] Defendant's Website tracks and transmits data via first-party and third-party cookies. The c_user cookie or Facebook ID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers. Google Analytics uses a UserID (uid) cookie to track a unique user across multiple devices, while Google DoubleClick uses DSID and IDE cookies for the same purposes.

137. Google's _ga and _gid cookies, also utilized by Defendant's Google Tracking Technologies, function similarly to Facebook's _fbp cookie.

138. The Meta Pixel and Google Analytics use both first- and third-party cookies, and both were used on the Website.[64]

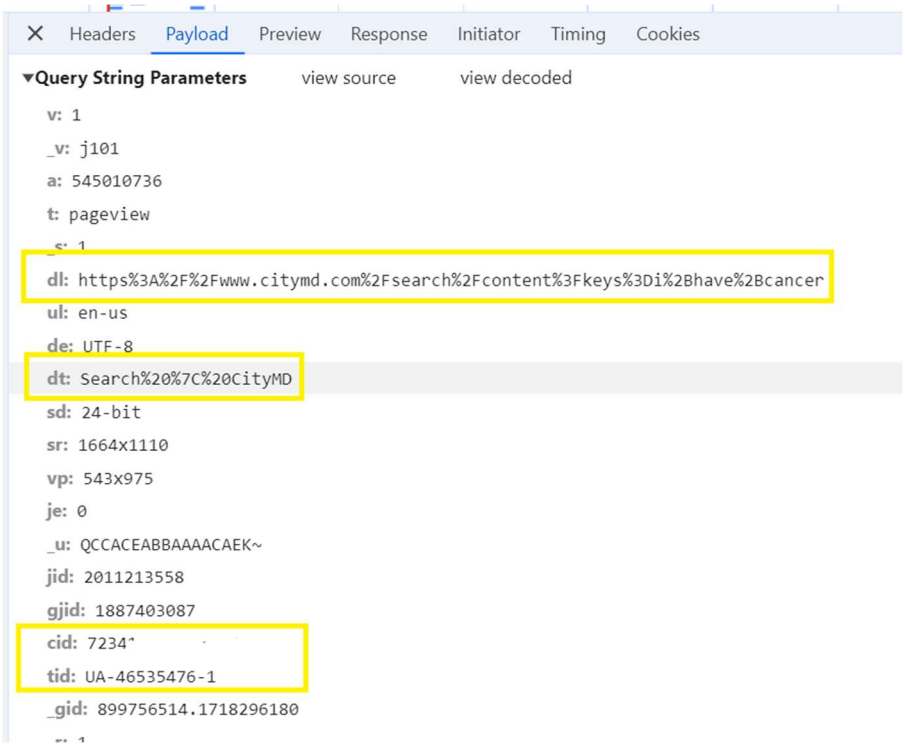
139. In addition, Plaintiffs' counsel's research shows that by July 2021 or earlier CityMD had enabled Automatic Setup and Advanced Matching on its Meta Pixel. Automatic Setup caused its Meta Pixel to transmit 'Microdata' and 'SubscribedButtonClick' events to Facebook, which carry a wealth of information about a patient's activity on the Website. CityMD had configured Advanced Matching to transmit a patient's email, first name, last name, gender, phone, country, state, and zip code to Facebook, as they entered this PII into forms on the Website along with their PHI.

140. At present, the full breadth of Defendant's tracking and data sharing practices is unclear, but evidence suggests Defendant is using additional tracking pixels and tools to transmit its patients' Private Information to additional third parties. For example, the image below indicates that Defendant is also sending its patients' protected health information to Google via Google Analytics:

Figure 15. Screenshot of Google Analytics code, depicting Defendant's unique Google identifier ("tid= UA-465e35476-1"), the user's unique identifier ("cid"),[65] and the specific search the user made on the Website.

[64] A first-party cookie is "created by the website the user is visiting"—in this case, Defendant's Website. A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook. The _fbp cookie is always transmitted as a first-party cookie. At a minimum, Facebook uses the fr, _fbp, and c_user cookies to link website visitors' data to their Facebook IDs and corresponding accounts.

[65] The *cid* has been redacted to protect the user's identity.



141. The images above contain the user's search phrase ("I have cancer"), thereby revealing the user's status as a patient and that the patient is seeking treatment for cancer.

142. Defendant also does not appear to have enabled the IP address anonymization feature provided by Google Analytics because the text "aip:" does not appear in the Website Source Code, and therefore Google receives patients' communications alongside the patients' identifiers including their IP address, which is also personally identifiable and impermissible under HIPAA.

143. CityMD was also capturing and disclosing the Users' activity via LinkedIn tracking tools the moment they entered the CityMD Website.

144. CityMD embedded the LinkedIn Insight Tag that on the Website, which intercepted and recorded "click" events, among other categories of user data. "Click" events detail information about which page on the Website the user was viewing as well as the selections they were making.

145. These interceptions also included the li_sugr and lms_ads cookies, which LinkedIn utilizes to identify its account holders for targeted advertising.[66]

146. Utilizing through the LinkedIn Insight Tag and LinkedIn cookies, CityMD collected and disclosed sensitive PII and PHI from its users, including the patient's appointment time, who the appointment was for, their medical reason for booking the appointment, and their gender.

147. Therefore, Defendant intercepted its patients' and potential patients' Private Information including details of their medical appointments and transmitted this health information to LinkedIn without their consent.

148. Defendant does not disclose that the Meta Pixels, Google Analytics, LinkedIn Insight Tag, or any other Tracking Technologies embedded in the Website's Source Code track, record, and transmit Plaintiffs' and Class Members' Private Information to Facebook, Google and LinkedIn. Moreover, Defendant never received consent or written authorization to disclose Plaintiffs' and Class Members' private communications to Facebook, Google and/or LinkedIn.

G. Defendant's Conduct Is Unlawful and Violated Industry Norms.

i. Defendant Violated its own Privacy Policy.

149. Defendant's Website Privacy Policy states, "[w]hen you browse our website, you do so anonymously, unless you have previously indicated that you wish CityMD to remember your login and password or you submit a registration form. We do not collect personal information for the purpose of reselling or distributing that information."[67]

---

[66] *See* LINKEDIN COOKIE TABLE, https://www.linkedin.com/legal/l/cookie-table (last visited Jan. 16, 2025).

[67] *See* https://www.citymd.com/privacy ("Personal information means any information that may be used to identify an individual, including, but not limited to, a first and last name, email address, a home, postal or other physical address, other contact information, title, birth date, gender,

150. Defendant's Privacy Policy is clear that CityMD "will require your affirmative action to indicate your consent before we use your information for purposes other than the purpose for which it was submitted."[68]

151. Defendant's Privacy Policy further promises that "[y]our personal information is never shared outside CityMD without your permission, except under conditions explained below." Those conditions–none of which apply here–include sharing updates on new products, sharing news about software updates, and where it is required by law.[69]

152. Defendant violated its own Privacy Policy by unlawfully disclosing Plaintiffs' and Class Members' Private Information to Facebook, Google, LinkedIn, and likely other third parties without written authorization.

153. Defendant further violated its own Privacy Policy by misrepresenting the scope and purpose of its use of cookies and tracking technologies on its website. The Privacy Policy claims that cookies are used "to determine the usefulness of [CityMD's] website information" and "to see how effective [CityMD's] navigational structure is in helping users reach that information."[70] But Defendant installed tracking technologies, including Facebook Pixel and Google Analytics, that were not limited to analyzing the efficacy of website navigation and were instead designed to collect, monetize, and transmit users' data to third parties for advertising and marketing purposes.

154. Defendant also represents that users could navigate its website anonymously or opt out of tracking technologies but goes on to say that certain portions of its website are inaccessible

---

occupation, industry, personal interests, medical conditions or other information when needed to provide a service you requested.") (last visited Jan. 14, 2025).

[68] *Id.*

[69] *Id.*

[70] *Id.*

without accepting cookies and tracking technologies.[71] This left Plaintiffs and Class Members with no meaningful choice but to subject themselves to invasive tracking and data collection practices, which undermines the very premise of anonymity promised in the Privacy Policy.

155. Defendant's claim that users could manage cookies and tracking technologies on their own devices shifts the burden of privacy protection to consumers rather than fulfilling Defendant's obligation to safeguard sensitive information. This is particularly egregious given that Defendant is a healthcare provider entrusted with the protected health information of Plaintiffs and Class Members, information that is safeguarded under HIPAA and should not be disclosed to third parties for marketing purposes without explicit consent.

156. Protected health information is further governed by Defendant's Notice of Privacy Practices.

157. Defendant's Notice of Privacy Practices explicitly explains "[h]ow medical information about you may be used and disclosed."[72] In this Notice, Defendant expressly maintains that "[u]ses and disclosures [of PHI] for marketing purposes" are to "be made only with your authorization."

158. At no point did CityMD seek such authorization from Plaintiffs before transmitting protected health information to a third party for marketing purposes.

---

[71] *Id.*

[72] *See Notice of Privacy Practices* (last updated Feb. 1, 2019), https://www.citymd.com/sites/default/files/2022-06/citymd-nj-ny-npp-2022.pdf (last visited Jan. 14, 2025).

159. Defendant's Notice of Privacy Practices further allows that "[y]ou have the right to request a restriction of your protected health information."[73] This language reflects Defendant's awareness of the high value patients such as Plaintiffs and Class Members place on their PHI.

160. Defendant's transmission of PHI to third parties such as Facebook or Google violated its own Notice of Privacy Practices, in which CityMD acknowledges that "[w]e are required to abide by the terms of this Notice of Privacy Practices."[74]

ii. Defendant Violated HIPAA Standards.

161. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient or household member of a patient for marketing purposes without the patients' express written authorization.[75]

162. The HIPAA Privacy Rule "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[76]

163. The Privacy Rule broadly defines "protected health information" ("PHI") as individually identifiable health information ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

---

[73] *Id.*

[74] *Id.*

[75] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502, 164.508(a)(3), 164.514(b)(2)(i).

[76] *HIPAA For Professionals*, https://www.hhs.gov/hipaa/for-professionals/index.html (last visited Jan. 14, 2025).

164. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

165. Under the HIPAA de-identification rule, "health information is not individually identifiable health information only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed":

A. Names;

….

H. Medical record numbers;

….

J. Account numbers;

….

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

O. Internet Protocol (IP) address numbers; … and

R. Any other unique identifying number, characteristic, or code…; and

The covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an

individual who is a subject of the information."[77]

166. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

167. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual." The statute states that a "person … shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320d-6.

168. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

169. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties.[78] There is a penalty enhancement where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall "be fined not more than $250,000, imprisoned not more than 10 years, or both."

[77] 45 C.F.R. § 164.514(b).

[78] 42 U.S.C. § 1320d-6(b)

170. In its *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule*, the HHS instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[79]

171. In its guidance for marketing, HHS further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*.[80]

172. As described above, the OCR addresses the obligations of "regulated entities," which are HIPAA-covered entities and business associates, when using tracking technologies.[81]

173. The Bulletin expressly provides that **"[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI**

[79] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Jan. 14, 2025) (emphasis added).

[80] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited Jan. 14, 2025).

[81] *See* OCR Bulletin *supra, note 19*.

to tracking technology vendors or any other violations of the HIPAA Rules." (emphasis in original).

174. As such, Defendant's actions violated HIPAA.

H. Plaintiffs' and Class Members' Reasonable Expectation of Privacy.

175. Plaintiffs and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

176. Indeed, at all times when Plaintiffs and Class Members provided their Private Information to Defendant, they each had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

177. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative consent before a company collects and shares its customers' data to be one of the most important privacy rights.

178. For example, a Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[82]

179. Personal data privacy and obtaining consent to share Private Information are material to Plaintiffs and Class Members.

180. Plaintiffs and Class Members would not have used Defendant's Website, would not have provided their Private Information to Defendant and would not have paid for Defendant's

[82] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-lessconfident-about-healthcare-data-privacy-and-car-safety-a3980496907/ (last visited Jan. 12, 2025).

healthcare services or would have paid less for them, had they known that Defendant would disclose their Private Information to third parties.

181. Plaintiffs' and Class Members' reasonable expectations of privacy in their PII/PHI are grounded in, among other things, Defendant's status as a healthcare provider, Defendant's common law obligation to maintain the confidentiality of patients' PII/PHI, state and federal laws protecting the confidentiality of medical information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification and Defendant's express and implied promises of confidentiality.

J. CityMD Was Enriched and Benefitted from the Use of the Tracking Technologies and Unauthorized Disclosures.

182. One of the primary reasons that Defendant decided to embed the Pixel and other Tracking Technologies on its Website was to commit criminal and tortious acts in violation of federal and state laws as alleged herein, namely, the use of patient data in the absence of express written consent.

183. Defendant's disclosure of the Private Information after the initial interception, including for marketing and revenue generation, was in violation of HIPAA and an invasion of privacy.

184. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook, Google and LinkedIn in the form of enhanced advertising services and more cost-efficient marketing.

185. Retargeting is a form of online marketing that targets users with ads based on their previous Internet communications and interactions.

186. The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a health care website back to Facebook, Google and/or LinkedIn via the Tracking Technologies embedded on, in this case, Defendant's Website.

187. For example, when a user searches for an urgent care location on the Website, that information is sent to Facebook. Facebook can then use its data on the user to find more users to click on a CityMD ad and ensure that the users targeted are more likely to convert.[83]

188. Through this process, the Pixel loads and captures as much data as possible when a user loads a telehealth website that has installed the Pixel. The information the Pixel captures, "includes URL names of pages visited, and actions taken—all of which could be potential examples of health information."[84]

189. As part of its marketing campaign, Defendant re-targeted patients and potential patients to get more visitors to its Website to use its services. Defendant did so through use of the intercepted patient data it obtained, procured and/or disclosed in the absence of express written consent.

190. Companies have started to warn about the potential HIPAA violations associated with using pixels and tracking technologies because many such trackers are not HIPAA-compliant or are only HIPAA-compliant if certain steps are taken.[85]

---

[83] *See How to Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking* (Mar. 14, 2023), https://www.freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliantand-still-get-conversion-tracking (last accessed Jan. 14, 2025).

[84] *Id.*

[85] *See The guide to HIPAA compliance in analytics*, https://campaign.piwik.pro/wpcontent/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf (explaining that Google Analytics 4 is not HIPAA-compliant) (last accessed June 4, 2024).

191. For example, Freshpaint, a healthcare marketing vendor, cautioned that "Meta isn't HIPAA-compliant. They don't sign BAAs, and the Meta Pixel acts like a giant personal user data vacuum sending PHI to Meta servers," and "[i]f you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now.[86]

192. Medico Digital also warns that "retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences."[87]

193. By utilizing the Tracking Technologies, the cost of advertising and retargeting was reduced through further use of the unlawfully intercepted and disclosed Private Information, thereby benefitting Defendant while invading the privacy of Plaintiffs and Class Members and violating their rights under federal and New York law.

K. Plaintiffs' and Class Members' Private Information Had Financial Value.

194. Plaintiffs' Private Information has economic value and Defendant's disclosures harmed Plaintiffs and Class Members.

195. Facebook regularly uses the data that it acquires to create Core and Custom Audiences as well as Lookalike Audiences and then sells that information to advertising clients.

196. Plaintiffs' and Class Members' Private Information has considerable value as highly monetizable data especially insofar as it allows companies to gain insight into their customers so that they can perform targeted advertising and boost their revenues.

---

[86] *How To Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking*, *supra* note 66.

[87] The complex world of healthcare retargeting (July 10, 2023), https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting (last accessed June 4, 2024).

197. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes: "Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information."[88]

198. Various reports have been conducted to identify the value of health data. For example, in 2023, the Value Examiner published a report entitled Valuing Healthcare Data. The report focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of "such data should ensure it is priced at fair market value to mitigate any regulatory risk."[89]

199. Trustwave Global Security also published a report entitled The Value of Data. With respect to healthcare data records, the report found that they may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[90]

200. The value of health data has also been reported extensively in the media. For example, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data

---

[88] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004).

[89] *See* https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf (last visited Jan. 15, 2025).

[90] *See* https://www.imprivata.com/blog/healthcare-data-new-prize-hackers (citing https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf) (last visited Jan. 12, 2025).

has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[91]

201. Similarly, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[92]

202. Indeed, numerous marketing services and consultants offering advice to companies on how to build their email and mobile phone lists—including those seeking to take advantage of targeted marketing—direct putative advertisers to offer consumers something of value in exchange for their personal information. "No one is giving away their email address for free. Be prepared to offer a book, guide, webinar, course or something else valuable."[93]

203. There is also a market for data in which consumers can participate. Personal information has been recognized by courts as extremely valuable. *See, e.g.*, *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig*., 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

---

[91] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Jan. 12, 2025).

[92] *See* https://time.com/4588104/medical-data-industry/ (last visited Jan. 12, 2025)

[93] VERO, HOW TO COLLECT EMAILS ADDRESSES ON TWITTER https://www.getvero.com/resources/twitter-lead-generation-cards/ (last visited Jan. 12, 2025).

204. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiffs herein can sell or monetize their own data.

205. Several companies, such as Google, Nielsen, UpVoice, HoneyGain and SavvyConnect, have products through which they pay consumers for a license to track their data.[94]

206. Facebook has also paid users for their digital information, including browsing history. Until 2019, Facebook ran a "Facebook Research" app through which it paid $20 a month for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

207. Additionally, healthcare data is extremely valuable to bad actors. Health care records may be valued at up to $250 per record on the black market.[95]

208. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

209. Healthcare data is incredibly valuable because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been sold. Once it has been detected, it can take years to undo the damage caused.

210. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

---

[94] *See 10 Apps for Selling Your Data for Cash*, https://wallethacks.com/apps-for-selling-your-data/ (last accessed Jan 15, 2025).

[95] Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data, SecureLink* (June 30, 2021), https://www.imprivata.com/blog/healthcare-data-new-prize-hackers (last accessed Jan. 15, 2025).

211. Defendant gave away Plaintiffs' and Class Members' communications and transactions on its Website without permission.

212. The unauthorized access to Plaintiffs' and Class Members' personal and Private Information has diminished the value of that information, resulting in harm to Website users, including Plaintiffs and Class Members.

REPRESENTATIVE PLAINTIFFS' EXPERIENCES

PLAINTIFF V.A.

213. As a condition of receiving Defendant's services, Plaintiff V.A. disclosed her Private Information to Defendant on numerous occasions, and most recently around October 2021.

214. Plaintiff V.A. accessed Defendant's Website on her phone and computer to research and provide information regarding the healthcare services she received from Defendant.

215. Plaintiff V.A. used Defendant's services to request and book doctor's appointments for herself as well as review her medical records and access Defendant's patient portal.

216. During the relevant time period, Plaintiff V.A. used Defendant's Website to research symptoms, testing, and diagnosis for both Covid-19 and the flu and other sensitive health conditions and to search for Defendant's locations close to her address. Her searches for information related to Covid-19 and the flu included her visiting specific webpages that revealed her PHI through the URLs as well as searches through the Website's search bar that disclosed the specific phrases that she used to search for information related to her medical conditions.

217. The full scope of Defendant's interceptions and disclosures of Plaintiff's communications to Meta, Google, LinkedIn and likely other third parties can only be determined through formal discovery. However, in addition to disclosing the specific searches Plaintiff entered into the Website's search bar, Defendant intercepted at least the following communications about

Plaintiff's patient status, medical conditions (including her treatment and diagnosis of Covid-19 and the flu), treatments sought, and the locations for receipt of healthcare, via the following long-URLs or substantially similar URLs that were sent to Meta via the Pixel (and which contain information concerning Plaintiff's specific medical conditions, queries, and treatments sought:

- https://citymd.com/services/lab-tests-screenings/covid-19-testing
- https://citymd.com/services/illnesses/cold-flu
- https://citymd.com/urgent-care-locations
- https://www.citymd.com/urgent-care-locations/ny/east-50th
- https://www.citymd.com/urgent-care-locations/ny/east-37th

218. Plaintiff V.A. has used and continues to use the same devices to maintain and access active Facebook, Google and LinkedIn accounts throughout the relevant period in this case.

219. Plaintiff V.A. reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

220. However, as a result of the Tracking Technologies Defendant chose to install on its Website, Plaintiff V.A.'s Private Information was intercepted, viewed, analyzed and used by unauthorized third parties.

221. Defendant transmitted Plaintiff V.A.'s unique identifiers including her Facebook ID, Google user ID and LinkedIn identifiers, computer IP address and other device and unique online identifiers to third parties like Facebook, Google, and LinkedIn. Defendant also transmitted information such as health and medical information including Plaintiff's particular health condition, the type of medical treatment sought, patient status and the fact that Plaintiff attempted to or did book a medical appointment.

222. Plaintiff V.A. never consented to the disclosure of or use of her Private Information by third parties or to Defendant enabling third parties to access or interpret such information. Plaintiff V.A. never consented to any third parties' receipt or use of her Private Information.

223. Notwithstanding, through the Tracking Technologies embedded on Defendant's Website, Defendant transmitted Plaintiff V.A.'s Private Information to, at a minimum, Facebook, Google, LinkedIn and likely other third parties.

224. As a result, Plaintiff V.A. received targeted ads on Facebook or Instagram inviting her to visit other CityMD urgent care locations, even after she had made use of their services, as well as ads related to Covid-19.

225. By making these disclosures without her consent, Defendant breached Plaintiff Andretta's privacy and unlawfully disclosed her Private Information.

226. Defendant did not inform Plaintiff V.A. that it had shared her Private Information with Facebook, Google, LinkedIn and any other third parties.

227. Plaintiff V.A. has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future unauthorized disclosure(s).

PLAINTIFF T.G.

228. As a condition of receiving Defendant's services, Plaintiff T.G. disclosed her Private Information to Defendant on numerous occasions from approximately 2020 through 2024.

229. Plaintiff T.G. accessed Defendant's Website on her phone and computer to book appointments and look up medical information.

230. Plaintiff T.G. used Defendant's services to request and book doctor's appointments for herself.

231. During the relevant time period, Plaintiff T.G. used Defendant's Website to research symptoms, testing, and diagnosis for Covid symptoms, ear infection symptoms, and flu symptoms and other sensitive health conditions and to search for Defendant's locations close to her address. Her searches for information related to Covid-19 and the flu included her visiting specific webpages that revealed her PHI through the URLs as well as searches through the Website's search bar that disclosed the specific phrases that she used to search for information related to her medical conditions.

232. The full scope of Defendant's interceptions and disclosures of Plaintiff T.G.'s communications to Meta, Google, LinkedIn, and other third parties can only be determined through formal discovery. However, in addition to disclosing specific searches Plaintiff T.G. entered into the Website's search bar, Defendant intercepted communications about Plaintiff's patient status, medical conditions, treatments sought, and locations for healthcare.

233. Plaintiff T.G. has used and continues to use the same devices to maintain and access active Facebook and Google accounts throughout the relevant period.

234. Plaintiff T.G. reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

235. However, as a result of the Tracking Technologies Defendant chose to install on its Website, Plaintiff T.G.'s Private Information was intercepted, viewed, analyzed, and used by unauthorized third parties.

236. Defendant transmitted Plaintiff T.G.'s unique identifiers, including Facebook ID, Google user ID, computer IP address, and other device and unique online identifiers to third parties like Facebook and Google. Defendant also transmitted information such as health and medical

information, including Plaintiff T.G.'s particular health conditions, the type of medical treatment sought, patient status, and the fact that Plaintiff attempted to or did book a medical appointment.

237. Plaintiff T.G. never consented to the disclosure or use of her Private Information by third parties, nor did she consent to Defendant enabling third parties to access or interpret such information.

238. Notwithstanding, through the Tracking Technologies embedded on Defendant's Website, Defendant transmitted Plaintiff T.G.'s Private Information to, at a minimum, Facebook, Google, LinkedIn, and likely other third parties.

239. As a result, Plaintiff T.G. received targeted ads on Facebook and Instagram inviting her to visit other CityMD urgent care locations, even after she had made use of their services, as well as ads related to her specific health conditions.

240. By making these disclosures without her consent, Defendant breached Plaintiff T.G.'s privacy and unlawfully disclosed her Private Information.

241. Defendant did not inform Plaintiff T.G. that it had shared her Private Information with Facebook, Google, LinkedIn, or any other third parties.

242. Plaintiff T.G. has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future unauthorized disclosure(s).

TOLLING

243. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiffs did not know (and had no way of knowing) that their PII and/or PHI was intercepted and unlawfully disclosed to Facebook, Google, LinkedIn and potentially other third parties

because Defendant kept this information secret. Alternatively, applicable statutes of limitations have been tolled by other applicable rules or doctrines.

CLASS ACTION ALLEGATIONS

244. Plaintiffs T.G. and V.A. bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class") pursuant to Rule 23(b)(2), 23(b)(3) and 23(c)(4) of the Federal Rules of Civil Procedure.

245. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals residing in the United States who used the CityMD Website and whose confidential personally identifiable information ("PII") and protected health information ("PHI") were shared with third parties through tracking technologies on CityMD's Website.

246. The New York Sub-Class that Plaintiffs seek to represent is defined as:

> All individuals residing in the State of New York who used the CityMD Website and whose confidential personally identifiable information ("PII") and protected health information ("PHI") were shared with third parties through tracking technologies on CityMD's Website.

247. The Nationwide Class and New York Sub-Class are collectively referred to as the "Class" unless otherwise and more specifically identified.

248. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

249. Plaintiffs reserve the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

250. Numerosity, Fed R. Civ. P. 23(a)(1). The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds of

thousands of individuals whose PII and PHI may have been improperly disclosed to Facebook, and the Class is identifiable within Defendant's records.

251. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant adequately, promptly and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;

d. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

e. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;

f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;

g. Whether Plaintiffs and Class Members are entitled to actual, consequential and/or nominal damages as a result of Defendant's wrongful conduct; and

h. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their Private Information.

252. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's incorporation of the tracking technologies, due to Defendant's misfeasance.

253. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

254. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

255. Policies Generally Applicable to the Class. Fed. R. Civ. P. 23(b)(2). This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to

ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

256. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

257. The litigation of the claims is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

258. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

259. Unless a class-wide injunction is issued, Defendant may continue disclosing the Private Information of Class Members, Defendant may continue to refuse to provide proper

notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint.

260. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

261. Issue Certification, Fed. R. Civ. P. 23(c)(4). Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to, the following:

a. Whether Defendant owed a legal duty to not disclose Plaintiffs' and Class Members' Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;

f. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I

VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT 18 U.S.C. § 2511(1), *et seq*. UNAUTHORIZED INTERCEPTION, USE AND DISCLOSURE (*On Behalf of Plaintiffs & the Nationwide Class*)

262. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

263. The ECPA prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

264. The ECPA protects both sending and receipt of communications.

265. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

266. The transmissions of Private Information to Defendant via Defendant's Website qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

267. The transmissions of Plaintiffs' Private Information to medical professionals qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(2).

268. **Electronic Communications**. The transmission of Private Information between Plaintiffs and Class Members and Defendant via its Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or

photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

269. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] *any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

270. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

271. **Electronic, Mechanical, or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5).

272. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The cookies Defendant and third parties, such as Meta, Google, and LinkedIn use to track Plaintiffs' and Class Members' communications;

b. Plaintiffs' and Class Members' browsers;

c. Plaintiffs' and Class Members' computing devices;

d. Defendant's web-servers; and

e. The Tracking Technologies deployed by Defendant to effectuate the sending and acquisition of patient communications.

273. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Tracking Technologies embedded and operating on its Website, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of

Plaintiffs' and Class Members' electronic communications to third parties, including Facebook, Google and LinkedIn, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c).

274. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Tracking Technologies embedded and operating on its Website, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiffs' and Class Members' electronic communications, for purposes other than providing health care services to Plaintiffs and Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(d).

275. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Tracking Technologies it embedded, configured and operated on its Website, contemporaneously and intentionally disclosed the contents of Plaintiffs' and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook, Google and LinkedIn.

276. Defendant's intercepted communications include, but are not limited to, the contents of communications to and/or from Plaintiffs' and Class Members' regarding PII and PHI, treatment, scheduling details and bill payments.

277. Additionally, through the above-described Tracking Technologies and intercepted communications, this information was, in turn, used by third parties, such as Facebook, to (1) place

Plaintiffs in specific health-related categories and (2) target Plaintiffs with advertising associated with Plaintiffs' specific health conditions.

278. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

279. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

280. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Tracking Technologies to track and utilize Plaintiffs' and Class Members' PII and PHI for financial gain.

281. Defendant was not acting under color of law to intercept and disclose Plaintiffs' and Class Members' wire or electronic communication.

282. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of disclosing those communications to third parties in violation of HIPAA and invading Plaintiffs' privacy via the Tracking Technologies.

283. Any purported consent that Defendant received from Plaintiffs and Class Members was not valid.

284. **Unauthorized Purpose**. Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a

tortious or criminal act in violation of the Constitution or laws of the United States or of any State, such as New York—namely, to disclose that interception in violation of HIPAA and invasion of privacy, among others.

285. **Any party exception in 18 U.S.C. § 2511(2)(d) does not apply.** The party exception in § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State.

286. Defendant is a "party to the communication" with respect to patient communications. However, Defendant's simultaneous, unknown duplication, forwarding and disclosure of Plaintiffs' and Class Members' Private Information does not qualify for the party exemption.

287. Here, as alleged above, Defendant violated provision 42 U.S.C. § 1320d-6(a)(3) of the Health Insurance Portability and Accountability Act. This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information (IIHI) to a third party. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) ***relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual***, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[96]

288. Plaintiffs' information that Defendant disclosed to third parties qualifies as IIHI, and Defendant violated Plaintiffs' expectations of privacy, and constitutes tortious and/or criminal

[96] § 1320d-(6) (emphasis added).

conduct through a violation of 42 U.S.C. § 1320d(6). Defendant used the wire or electronic communications to increase its profit margins. Defendant specifically used the Tracking Technologies to track and utilize Plaintiffs' and Class Members' PII and PHI for financial gain.

289. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

290. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it:

a. Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and

b. Disclosed IIHI to Facebook, Google and LinkedIn without patient authorization.

291. Defendant's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant's use of the Facebook, Google, LinkedIn, and other third parties' source code was for Defendant's commercial advantage to increase revenue from existing patients and gain new patients.

292. Healthcare patients have the right to rely upon the promises that companies make to them. Defendant accomplished its tracking and retargeting through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that cause Facebook pixels and cookies (including but not limited to the _fbp, _ga and cid cookies) and other tracking technologies to be deposited on Plaintiffs' and Class Members' computing devices as "first-party" cookies that are not blocked.

293. The _fbp, _ga, and cid cookies, commanded Plaintiffs' and Class Members' computing devices to redirect and disclose their data and the content of their communications with Defendant to Google, Facebook, LinkedIn and others.

294. Defendant knew or had reason to know that the _fbp, _ga, and cid cookies would command Plaintiffs' and Class Members' computing devices to remove, redirect and disclose their data and the content of their communications with Defendant to Google, Facebook, LinkedIn and others.

295. Defendant's scheme or artifice to defraud in this action consists of: (a) the false and misleading statements and omissions in its privacy policy (HIPAA Notice) set forth above, including the statements and omissions recited in the claims below and (b) the placement of the '_fbp,' "_ga," and "cid" cookies on patient computing devices disguised as a first-party cookie on Defendant's Website rather than a third-party cookie from Meta or Google.

296. Defendant acted with the intent to defraud in that it willfully invaded and took Plaintiffs' and Class Members' property rights (a) to the confidentiality of Private Information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes and (b) to determine who has access to their computing devices.

297. As such, Defendant cannot viably claim any exception to ECPA liability.

298. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their individually identifiable patient health information (including information about their medical symptoms, conditions, treatments and concerns, medical appointments, healthcare providers and locations, health insurance and medical bills) for commercial purposes has caused Plaintiffs and the Class Members to suffer emotional distress;

b. Defendant received substantial financial benefits from its use of Plaintiffs' and Class Members' PII and/or PII without providing any value or benefit to Plaintiffs or the Class Members;

c. Defendant received substantial, quantifiable value from its use of Plaintiffs' and Class Members' PII and/or PHI, such as understanding how people use its website and determining what ads people see on its website, without providing any value or benefit to Plaintiffs or the Class Members;

d. Defendant has failed to provide Plaintiffs and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information; and

e. The diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, test results, and appointments that Plaintiffs and Class Members intended to remain private no longer private.

299. As a result of Defendant's violation of the ECPA, Plaintiffs and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT II

BREACH OF IMPLIED CONTRACT
(on behalf of Plaintiffs & the Nationwide Class, or Alternatively, the New York Subclass)

299. Plaintiffs repeat and re-allege every allegation contained in the Complaint as if fully set forth herein.

300. As a condition of utilizing Defendant's Website and receiving services from Defendant's healthcare facilities and professionals, Plaintiffs and the Class Members provided their Private Information and compensation for their medical care.

301. When Plaintiffs and Class Members provided their Private Information to Defendant, they entered an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

302. Plaintiffs and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

303. Plaintiffs and Class Members would not have retained Defendant to provide healthcare services in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

304. Defendant breached these implied contracts by disclosing Plaintiffs' and Class Members' Private Information without consent to third parties like Facebook or Google.

305. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged herein, including but not limited to the loss of the benefit of their bargain and diminution in value of Private Information.

306. Plaintiffs and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

COUNT III

NEGLIGENCE
(*On behalf of Plaintiffs & the Nationwide Class, or Alternatively, the New York Subclass*)

307. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

308. Defendant owed Plaintiffs and Class Members a duty to keep their Private Information completely confidential, and to safeguard sensitive personal and medical information.

309. Plaintiffs and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

310. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed its Tracking Technologies to disclose and transmit to third parties Plaintiffs' and Class Members' communications with Defendant, including Private Information and the contents of such information.

311. These disclosures were made without Plaintiffs' or Class Members' knowledge, consent, or authorization, and were unprivileged.

312. The third-party recipients included, but may not be limited to, Facebook, Google and/or LinkedIn.

313. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiffs and Class Members were damaged by Defendant's breach in that:

a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;

b. Plaintiffs and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;

c. Defendant eroded the essential confidential nature of the provider-patient relationship;

d. General damages for invasion of their rights in an amount to be determined by a jury;

e. Nominal damages for each independent violation;

f. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensation for such data;

g. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

h. Defendant's actions diminished the value of Plaintiffs' and Class Members' Private Information; and

i. Defendant's actions violated the property rights Plaintiffs and Class Members have in their Private Information.

COUNT IV

BREACH OF CONFIDENCE
(*On Behalf of Plaintiffs & the Nationwide Class, or Alternatively, the New York Subclass*)

314. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

315. Possessors of non-public medical information, such as CityMD, have a duty to keep such medical information completely confidential.

316. Plaintiffs and Class Members had reasonable expectations of privacy in the responses and communications entrusted to CityMD through their Website, which included highly sensitive Private Information.

317. Contrary to its duties as a healthcare provider and its express promises of confidentiality, CityMD installed the Tracking Technologies to disclose and transmit to third parties Plaintiffs' and Class Members' Private Information, including data related to Plaintiffs' and Class Members' health.

318. These disclosures were made without Plaintiffs' or Class Members' knowledge, consent, or authorization.

319. The third-party recipients included, but may not be limited to, Facebook, Google, LinkedIn and likely other third parties.

320. As a direct and proximate cause of CityMD's unauthorized disclosures of Plaintiffs' and Class Members' Private Information, Plaintiffs and Class Members were damaged by CityMD's breach of confidentiality in that (a) sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private; (b) Plaintiffs and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements; (c) CityMD eroded the essential confidential nature of health services that Plaintiffs and Class Members participated in; (d) general damages for invasion of their rights in an amount to be determined by a jury at trial; (e) nominal damages for each independent violation; (f) the unauthorized use of something of value (the highly sensitive Private Information) that belonged to Plaintiffs and Class Members and the obtaining of a benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensation to Plaintiffs or Class Members for the unauthorized use of such data; (g) diminishment of the value

of Plaintiffs' and Class Members' Private Information; and (h) violation of the property rights Plaintiffs and Class Members have in their Private Information.

COUNT V

CONSTRUCTIVE BAILMENT
(*On Behalf of Plaintiffs & the Nationwide Class, or Alternatively, the New York Subclass*)

321. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

322. CityMD acquired and was obligated to safeguard the Private Information of Plaintiffs and Class Members.

323. CityMD accepted possession and took control of Plaintiffs' and Class Members' Private Information under such circumstances that the law imposes an obligation to safeguard the property of another.

324. CityMD accepted possession and took control of Plaintiffs' and Class Members' Private Information under such circumstances that the law imposes and obligation to safeguard the property of another.

325. Specifically, a constructive bailment arises when CityMD, as is the case here, takes lawful possession of the property of another and has a duty to account for that property, without intending to appropriate it.

326. Constructive bailments do not require an express assumption of duties and may arise from the bare fact of the thing coming into the actual possession and control of a person fortuitously or by mistake as to the duty of ability of the recipient to affect the purpose contemplated by the absolute owner.

327. During the bailment, CityMD owed a duty to Plaintiffs and Class Members to exercise reasonable care, diligence, and prudence in protecting their Private Information.

328. CityMD further breached its duty to safeguard Plaintiffs' and Class Members' Private Information had been disclosed to third parties without Plaintiffs' and Class Members' knowledge, consent, or explicit authorization.

329. As a direct and proximate cause of CityMD's breach of its obligations to safeguard their property, Plaintiffs and Class Members have suffered compensable damages that were reasonably foreseeable to CityMD, including but not limited to, the damages set forth herein.

COUNT VI

VIOLATION OF THE NEW YORK DECEPTIVE TRADE PRACTICES ACT NEW YORK GEN. BUS. LAW § 349, *ET SEQ.* (*On Behalf of Plaintiffs & the New York Subclass*)

330. Plaintiffs re-alleges and incorporate by reference the allegations above as if fully set forth herein.

331. By the facts and conduct alleged herein, CityMD committed unfair or deceptive acts and practices by:

a. Promising to maintain the privacy and security of Plaintiffs' and Class Members' PHI and/or PII as required by law;

b. Installing the Tracking Technologies to operate as intended and transmit Plaintiffs' and Class Members' Private Information without their authorization to Facebook, Google, LinkedIn and other third parties;

c. Failing to disclose or omitting material facts of Plaintiffs and Class Members regarding disclosure of their Private Information to Facebook, Google, LinkedIn and other third parties;

d. Failing to take proper action to ensure the tracking technologies were configured to prevent unlawful disclosure of Plaintiffs and Class Members' Private Information;

e. Unlawfully disclosing Plaintiffs' and Class Members' Private Information to Facebook, Google, LinkedIn and other third parties.

332. These unfair acts and practices violated duties imposed by laws, including but not limited to, the Federal Trade Commission Act, HIPAA and NY GBL § 349.

333. CityMD's actions also constitute deceptive and unfair acts or practices because CityMD knew it failed to disclose to Plaintiffs and the New York Class Members that their healthcare-related communications via the Website would be disclosed to Facebook, Google LinkedIn and other third parties.

334. CityMD's actions also constitute deceptive and unfair acts or practices because CityMD intended that Plaintiffs and the New York Class Members relied on its deceptive and unfair practices and the concealment and mission of material facts in connection with CityMD's offering of goods and services.

335. Specifically, CityMD was aware that Plaintiffs and the New York Class Members depended on and relied upon it to keep their communications confidential, and CityMD instead disclosed that information to Facebook, Google and LinkedIn.

336. In addition, CityMD's material failure to disclose that CityMD collects Plaintiffs' and the New York Class Members' Private Information for marketing purposes with Facebook, Google and LinkedIn constitutes an unfair act of practice prohibited by the NY GBL § 349. CityMD's actions were immoral, unethical, and unscrupulous.

337. Plaintiffs had reasonable expectations of privacy in their communications exchanged with CityMD, including communications exchanged via the Website.

338. Contrary to its duties as a medical provider and its express promises of confidentiality, CityMD deployed Tracking Technologies to disclose and transmit Plaintiffs' personally identifiable, non-public medical information and the contents of their communications exchanged with CityMD to third parties like Facebook, Google and LinkedIn.

339. CityMD's disclosures of Plaintiffs and the New York Class Members' Private Information were made without their knowledge, consent, or authorization, and were privileged.

340. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

341. CityMD willfully, knowingly, and intentionally and voluntarily engaged in the aforementioned acts when it incorporated the tracking technologies with knowledge of their purpose and functionality.

342. The harm described herein could not have been avoided by Plaintiffs and the New York Class Members through the exercise of ordinary diligence.

343. As a result of CityMD's wrongful conduct, Plaintiffs were injured in that they never would have provided their PII and/or PHI to CityMD or purchased CityMD's services, had they known or been told that CityMD shared confidential and sensitive Private Information with Facebook, Google and LinkedIn.

344. As a direct and proximate result of CityMD's multiple violations of the GBL § 349, Plaintiffs and the New York Class Members have suffered harm, including financial losses related to the payments or services made to CityMD that Plaintiffs and the New York Class Members would not have made had they known of CityMD's disclosure of their PII and/or PHI to Facebook,

Google, LinkedIn and other third parties, lost control over the value of their PII and/or PHI, including unwanted solicitations or marketing, entitling them to damages in an amount to be proven at trial.

345. CityMD's acts, practices, and omissions were done in the course of CityMD's business of furnishing healthcare-related services to consumers in the State of New York.

346. Plaintiffs bring this action on behalf of themselves and the New York Class Members, and are entitled to damages in an amount to be determined at trial, along with their costs and attorney's fees incurred in this action.

COUNT VII

INVASION OF PRIVACY
(*On behalf of Plaintiffs & the Nationwide Class, or Alternatively, the New York Subclass*)

347. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

348. A plaintiff asserting claims for intrusion upon seclusion must plead (1) that the defendant intentionally intruded into a place, conversation, or matter as to which plaintiff has a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

349. CityMD disclosure of Plaintiffs' and Class Members' sensitive data, including PII, health information, prescription requests and other interactions on the CityMD website, to third parties like Facebook, Google, and LinkedIn constitutes an intentional intrusion upon Plaintiffs' and Class Members' solitude or seclusion.

350. Plaintiffs and Class Members had a reasonable expectation of privacy in the health information and other personal data that CityMD disclosed to third parties. Plaintiffs' health information, prescription requests, and other interactions with the CityMD website are inherently

sensitive in nature. Plaintiffs and Class Members reasonably expected this information would remain private and confidential and would not be disclosed to third parties without their consent.

351. This expectation is especially heightened given CityMD consistent representations to users that this information would be safeguarded and not disclosed to third parties.

352. Plaintiffs and Class Members did not consent to, authorize, or know about CityMD's intrusion at the time it occurred. Accordingly, Plaintiffs and Class Members never agreed that CityMD could disclose their data to third parties.

353. The surreptitious disclosure of sensitive data, including PII and PHI from thousands of individuals was highly offensive because it violated expectations of privacy that have been established by social norms. Polls and studies show that the overwhelming majority of Americans believe one of the most important privacy rights is the need for an individual's affirmative consent before personal data is collected or shared.

354. The offensiveness of this conduct is all the more apparent because CityMD's disclosure of this information was conducted in secret in a manner that Plaintiffs and Class Members would be unable to detect, contrary to the actual representations made by CityMD.

355. As a result of CityMD actions, Plaintiffs and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

356. Plaintiffs and Class Members have been damaged as a direct and proximate result of CityMD's invasion of their privacy and are entitled to just compensation, including monetary damages.

357. Plaintiffs and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiffs and Class Members for the harm

to their privacy interests as well as a disgorgement of profits made by CityMD as a result of its intrusions upon Plaintiffs' and Class Members' privacy.

358. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of CityMD actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

359. Plaintiffs also seek such other relief as the Court may deem just and proper.

COUNT VIII

UNJUST ENRICHMENT
(*On behalf of Plaintiffs & the Nationwide Class*)

360. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

361. This claim is pleaded in the alternative to Plaintiffs' implied contract claim.

362. Defendant benefits from the use of Plaintiffs' and Class Members' Private Information and unjustly retained those benefits at their expense.

363. Plaintiffs and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiffs and Class Members, without authorization and proper compensation to exceed the limited authorization and access to that information which was given to Defendant.

364. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiffs and Class Members under the guise of keeping this information private. Defendant collected, used and disclosed this information for its own gain including for advertisement purposes, sale or trade for valuable services from third parties.

365. Plaintiffs and Class Members would not have used Defendant's services or would have paid less for those services, if they had known that Defendant would collect, use, and disclose this information to third parties.

366. Defendant exceeded any authorization given and instead consciously disclosed and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

367. Defendant unjustly retained those benefits at the expense of Plaintiffs and Class Members because Defendant's conduct damaged Plaintiffs and Class Members, all without providing any commensurate compensation to Plaintiffs and Class Members.

368. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members.

369. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

370. The benefits that Defendant derived from Plaintiffs and Class Members were not offered by Plaintiffs and Class Members gratuitously and rightly belong to Plaintiffs and Class Members. It would be against equity and good conscience for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts and trade practices alleged in this Complaint.

371. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs V.A. and T.G., on behalf of themselves and Class Members, requests judgment against CityMD and that the Court grant the following Order:

A. certifying the Class and appointing Plaintiffs and Counsel to represent such Class;

B. awarding equitable relief enjoining Defendant from engaging in the wrongful conduct alleged in this Complaint pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

C. awarding injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members:

D. awarding damages, including, but not limited to, actual, consequential, statutory, punitive, and nominal damages, as allowed by law in an amount to be determined;

E. awarding attorneys' fees, costs, and litigation expenses, as allowed by law;

F. awarding prejudgment interest on all amounts awarded; and

G. awarding such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiffs V.A. and T.J. hereby demand that this matter be tried before a jury.

LITE DEPALMA GREENBERG & AFANADOR, LLC

Dated: January 17, 2025

/s/ Joseph J. DePalma

Joseph J. DePalma
Catherine B. Derenze
570 Broad St., Ste. 1201
Newark, NJ 07102
Telephone: (973) 623-3000
Facsimile: (973) 623-0858
jdepalma@litedepalma.com
cderenze@litedepalma.com

STERLINGTON, PLLC
Jennifer Czeisler*
Edward Ciolko*
One World Trade Center, 85th Floor
New York, New York 10007
jen.czeisler@sterlingtonlaw.com
ed.ciolko@sterlingtonlaw.com

ALMEIDA LAW GROUP LLC
David S. Almeida*
Elena A. Belov*
849 W. Webster Avenue
Chicago, Illinois 60614
Tel: (312) 576-3024
david@almeidalawgroup.com
elena@almeidalawgroup.com

Attorneys for Plaintiffs and the Proposed Class

**Pro Hac Vice Forthcoming*

LOCAL CIVIL RULE 11.2 CERTIFICATION

Pursuant to Local Civil Rule 11.2, I hereby certify that the matter in controversy is not related to any other action, pending arbitration or administrative proceeding currently pending in any court.

I hereby certify that the following statements made by me are true. I am aware that if any of the foregoing statements made by me are willfully false, I am subject to punishment.

LITE DEPALMA GREENBERG & AFANADOR, LLC

Dated: January 17, 2025

/s/ Joseph J. DePalma

Joseph J. DePalma
Catherine B. Derenze
570 Broad St., Ste. 1201
Newark, NJ 07102
Telephone: (973) 623-3000
Facsimile: (973) 623-0858
jdepalma@litedepalma.com
cderenze@litedepalma.com

STERLINGTON, PLLC
Jennifer Czeisler*
Edward Ciolko*
One World Trade Center, 85th Floor
New York, New York 10007
jen.czeisler@sterlingtonlaw.com
ed.ciolko@sterlingtonlaw.com

ALMEIDA LAW GROUP LLC
David S. Almeida*
Elena A. Belov*
849 W. Webster Avenue
Chicago, Illinois 60614
Tel: (312) 576-3024
david@almeidalawgroup.com
elena@almeidalawgroup.com

Attorneys for Plaintiffs and the Proposed Class

**Pro Hac Vice Forthcoming*